

COMMUNICATIONS NETWORKS AND CONSUMER PRIVACY: RECENT DEVELOPMENTS

HEARING BEFORE THE SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY, AND THE INTERNET OF THE COMMITTEE ON ENERGY AND COMMERCE HOUSE OF REPRESENTATIVES ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

APRIL 23, 2009

Serial No. 111-31



Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE

72-880

WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON ENERGY AND COMMERCE

HENRY A. WAXMAN, California
Chairman

JOHN D. DINGELL, Michigan
Chairman Emeritus

EDWARD J. MARKEY, Massachusetts

RICK BOUCHER, Virginia

FRANK PALLONE, Jr., New Jersey

BART GORDON, Tennessee

BOBBY L. RUSH, Illinois

ANNA G. ESHOO, California

BART STUPAK, Michigan

ELIOT L. ENGEL, New York

GENE GREEN, Texas

DIANA DEGETTE, Colorado

Vice Chairman

LOIS CAPPS, California

MICHAEL F. DOYLE, Pennsylvania

JANE HARMAN, California

TOM ALLEN, Maine

JANICE D. SCHAKOWSKY, Illinois

HILDA L. SOLIS, California

CHARLES A. GONZALEZ, Texas

JAY INSLEE, Washington

TAMMY BALDWIN, Wisconsin

MIKE ROSS, Arkansas

ANTHONY D. WEINER, New York

JIM MATHESON, Utah

G.K. BUTTERFIELD, North Carolina

CHARLIE MELANCON, Louisiana

JOHN BARROW, Georgia

BARON P. HILL, Indiana

DORIS O. MATSUI, California

DONNA M. CHRISTENSEN, Virgin Islands

KATHY CASTOR, Florida

JOHN P. SARBANES, Maryland

CHRISTOPHER S. MURPHY, Connecticut

ZACHARY T. SPACE, Ohio

JERRY McNERNEY, California

BETTY SUTTON, Ohio

BRUCE BRALEY, Iowa

PETER WELCH, Vermont

JOE BARTON, Texas

Ranking Member

RALPH M. HALL, Texas

FRED UPTON, Michigan

CLIFF STEARNS, Florida

NATHAN DEAL, Georgia

ED WHITFIELD, Kentucky

JOHN SHIMKUS, Illinois

JOHN B. SHADEGG, Arizona

ROY BLUNT, Missouri

STEVE BUYER, Indiana

GEORGE RADANOVICH, California

JOSEPH R. PITTS, Pennsylvania

MARY BONO MACK, California

GREG WALDEN, Oregon

LEE TERRY, Nebraska

MIKE ROGERS, Michigan

SUE WILKINS MYRICK, North Carolina

JOHN SULLIVAN, Oklahoma

TIM MURPHY, Pennsylvania

MICHAEL C. BURGESS, Texas

MARSHA BLACKBURN, Tennessee

PHIL GINGREY, Georgia

STEVE SCALISE, Louisiana

SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY, AND THE INTERNET

RICK BOUCHER, Virginia

Chairman

EDWARD J. MARKEY, Massachusetts

BART GORDON, Tennessee

BOBBY L. RUSH, Illinois

ANNA G. ESHOO, California

BART STUPAK, Michigan

DIANA DeGETTE, Colorado

MICHAEL F. DOYLE, Pennsylvania

JAY INSLEE, Washington

ANTHONY D. WEINER, New York

G.K. BUTTERFIELD, North Carolina

CHARLIE MELANCON, Louisiana

BARON P. HILL, Indiana

DORIS O. MATSUI, California

DONNA M. CHRISTENSEN, Virgin Islands

KATHY CASTOR, Florida

CHRISTOPHER S. MURPHY, Connecticut

ZACHARY T. SPACE, Ohio

JERRY McNERNEY, California

PETER WELCH, Vermont

JOHN D. DINGELL, Michigan (*ex officio*)

FRED UPTON, Michigan

Ranking Member

J. DENNIS HASTERT, Illinois

CLIFF STEARNS, Florida

NATHAN DEAL, Georgia

BARBARA CUBIN, Wyoming

JOHN SHIMKUS, Illinois

HEATHER WILSON, New Mexico

CHARLES W. "CHIP" PICKERING,

Mississippi

VITO FOSELLA, New York

GEORGE RADANOVICH, California

MARY BONO MACK, California

GREG WALDEN, Oregon

LEE TERRY, Nebraska

MIKE FERGUSON, New Jersey

CONTENTS

	Page
Hon. Rick Boucher, a Representative in Congress from the Commonwealth of Virginia, opening statement	1
Hon. Cliff Stearns, a Representative in Congress from the State of Florida, opening statement	3
Hon. Anna G. Eshoo, a Representative in Congress from the State of California, opening statement	5
Hon. Mary Bono Mack, a Representative in Congress from the State of California, opening statement	6
Hon. George Radanovich, a Representative in Congress from the State of California, opening statement	7
Hon. Bart Stupak, a Representative in Congress from the State of Michigan, opening statement	7
Hon. Marsha Blackburn, a Representative in Congress from the State of Tennessee, opening statement	8
Hon. Edward J. Markey, a Representative in Congress from the Commonwealth of Massachusetts, prepared statement	10

WITNESSES

Leslie Harris, President, Chief Executive Officer, Center for Democracy and Technology	12
Prepared statement	15
Answers to submitted questions	138
Kyle McSillarow, President and CEO, National Cable and Telecommunications Association	30
Prepared statement	33
Answers to submitted questions	139
Marc Rotenberg, President and Executive Director, Electronic Privacy Information Center	40
Prepared statement	42
Answers to submitted questions	141
Dorothy Attwood, Senior Vice President, Public Policy and Chief Privacy Officer, AT&T Services, Inc.	52
Prepared statement	54
Answers to submitted questions	143
Ben Scott, Policy Director, Free Press	60
Prepared statement	62
Answers to submitted questions	149
Brian R. Knapp, Chief Operating Officer, Loopt, Inc.	86
Prepared statement	88
Answers to submitted questions	154
Richard Bennett, Publisher, Broadbandpolitics.com	96
Prepared statement	99
Answers to submitted questions	155

SUBMITTED MATERIAL

Statement of Scott Cleland, Precursor, LLC, submitted by Mr. Stearns	125
--	-----

COMMUNICATIONS NETWORKS AND CONSUMER PRIVACY: RECENT DEVELOPMENTS

THURSDAY, APRIL 23, 2009

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY,
AND THE INTERNET,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:05 a.m., in Room 2322 of the Rayburn House Office Building, Hon. Rick Boucher (chairman) presiding.

Members present: Representatives Boucher, Rush, Eshoo, Stupak, DeGette, Weiner, Christensen, Castor, Space, Stearns, Shimkus, Buyer, Radanovich, Bono Mack, Terry, and Blackburn.

Staff present: Roger Sherman, Chief Counsel; Tim Powderly, Counsel; Shawn Chang, Counsel; Greg Guice, Counsel; Amy Levine, Counsel, Sarah Fisher, Special Assistant; Pat Delgado, Chief of Staff Congressman Waxman; Neil Fried, Counsel; and Sam Costello, Legislative Clerk.

OPENING STATEMENT OF HON. RICK BOUCHER, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF VIRGINIA

Mr. BOUCHER. The subcommittee will come to order. Broadband networks are a primary driver of the national economy and it is fundamentally in the Nation's interest to encourage their expanded use. One clear way Congress can promote a greater use of the Internet for a variety of purposes including access to information, electronic commerce and entertainment is to assure Internet users of a higher degree of privacy protection with regard to data that is collected concerning their Internet usage. It is my intention for the subcommittee this year to develop on a bipartisan basis legislation extending to Internet users that assurance that their online experience is more secure. We see this measure as a driver of greater levels of Internet uses such as electronic commerce. Not as a hindrance to them.

Today's discussion is the first of two presently planned hearings relating to consumer privacy on electronic networks. Today we explore network-based privacy matters including the growing deployment of deep packet inspection technologies and location-based privacy enabled by specific technologies. There are additional privacy related matters that we intend to explore including targeted and behavioral advertising. And we are now planning to conduct a joint hearing with the full committee's Subcommittee on Commerce,

Trade and Consumer Protection during the early period of the summer in order to examine online privacy including behavioral advertising at which Internet-based companies will be invited to testify before the subcommittee.

A range of concerns related to online advertising should be vetted and just as there are concerns about the privacy implications of the network-based technologies upon which we are focusing this morning. Those online advertising concerns will be thoroughly vetted at the joint hearing we will have with the other subcommittee this summer. But today's focus is on emerging network technologies that have significant privacy implications and three of them will be highlighted by witnesses testifying to us today.

Deep packet inspection enables the opening of the packets which actually hold the content of Internet transported communications. Through the use of DPI, the content can be fully revealed and fully examined. It has generally been accepted that there are beneficial uses for DPI, such as enabling better control of networks and the blocking of Internet viruses and worms.

DPI also enables better compliance by Internet service providers with warrants authorizing electronic message intercepts by law enforcement, but its privacy intrusion potential is nothing short of frightening. The thought that a network operator could track a user's every move on the Internet, record the details of every search and read every e-mail or document attached to an e-mail message is alarming. And while I am certain that no one appearing on the panel today uses DPI in this manner, our discussion today of the capabilities of the technology and the extent of its current deployment, any projection that could be made about its anticipated schedule and path of deployment and the uses to which that technology is currently being put will give us as a subcommittee a better understanding of where to draw the lines between permissible and impermissible uses, or uses that might justify opt-in as opposed to opt-out consent from Internet users.

I look forward to hearing from our witnesses this morning about how we can best balance the deployment of DPI with adequate protection for consumers' privacy. For example, should a network operator's use of DPI always require opt-in consent or is opt-out sometimes appropriate and if so, under what circumstances would opt-out be appropriate? What services that consumers consider essential to the safe and effective functioning of the Internet are advanced through deep packet inspection?

Since the death of NebuAd, DPI-based behavioral advertising service last year, do we now see other companies using DPI in order to deliver behavioral advertising? What if any safeguards are in place to ensure that consumers are giving meaningful consent to the tracking of their activities on the Internet? These and other questions deserve our consideration this morning.

I also look forward to learning about other emerging network-based technologies such as Project Canoe on the cable platform and Loopt and the wireless-base employing new uses of cable set top boxes and GPS tracking capabilities on wireless devices. What benefits do these services offer to consumers and how should the network operator procure meaningful consent from users for their use?

We are also interested in hearing a preview of what the future of network-based technologies may hold. What new services may they enable and how do we accommodate with regard to them key privacy concerns? So I look forward to hearing from our distinguished panel and I want to thank each of our witnesses for appearing here this morning and sharing their expertise and views with the subcommittee.

At this time, I am pleased to recognize the Ranking Republican Member of the subcommittee, the gentleman from Florida, Mr. Stearns.

OPENING STATEMENT OF HON. CLIFF STEARNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Mr. STEARNS. Good morning and thank you, Mr. Chairman, and I appreciate your opening statement and you are offering a bipartisan tone to it, and your interest in having additional hearings including with the Commerce, Consumer Protection Trade which I chaired during Republican majority.

Our goal today should be to broadly examine how companies are using consumer Internet behavior to tailor online advertising, both the benefits to the consumers as well as any potential concerns that have not already been addressed by industry. Our focus should go beyond only broadband providers and also look at the entire Internet universe, including search engines and Internet advertising networks. We cannot have this discussion without addressing them, as well.

Whatever the appropriate standards are, they should apply to everyone. We need to be consistent. Consumers don't care if you are a search engine or a broadband provider. They just want to ensure that their privacy is protected.

I hope, Mr. Chairman, you will agree to hold more privacy hearings on this subcommittee and I am glad to hear that you will so that we hear from the network operators. That is the only way members can be fully informed about these issues before marking up any legislation.

As we move forward towards privacy legislation we must empower consumers to make their own privacy-related decisions. Only the consumer knows how he or she feels about the information that is being collected, the parties doing the collecting and the actual purpose for which the information will ultimately be used. Congress cannot and should not make that decision for them. We need to place the control over consumer information with the consumer himself. This means companies should be as transparent as possible about what information they collect and how do they use this information, that way consumers will be better able to make informed privacy decisions.

We also need to examine the ways in which the use of behavioral information for marketing has been shown to have already harmed consumers. It is imperative that there be some evidence of harm if we are going to regulate this practice or we run the risk of prematurely restricting the latest technological advancement related to online marketing.

Consumers' online activities provide advertisers with valuable platforms upon which to market their products, their services. Col-

lecting this type of information for targeted advertising is very important because it allows many of these products and services to remain free to consumers. Without this information, Web sites would either have to cut back on their free information and services or would have to start charging a fee to see to consumers. Neither result is good. Over-reaching privacy regulations, particularly in the absence of consumer harm, could have a significant negative economic impact at a time while many businesses in our economy are struggling. So let us look very closely at these issues before we leap to legislative proposals.

We also need a consumer-based approach. Consumers are the best judges. We will not truly address the privacy implications of tailored Internet advertising unless we shift the discussion towards consumer-centric approaches and away from the characteristics of the companies, like the particular technology they use or their corporate structure itself. Whatever we do, we must apply the same standards of privacy to companies collecting this type of information for the same type of purposes, whether it is a phone company, a cable company or companies like Google, Yahoo or Microsoft. Consumers don't care how their privacy has been invaded. What they care about is what the information is that is collected and how it is being used.

Now, Mr. Chairman, as you have mentioned, I have had a record of privacy when I was chairman of the trade and consumer protection subcommittee. We held the most extensive hearings on the topic of privacy and following these hearings I offered and introduced the Consumer Privacy Protection Act, which I hope will be used as a baseline for new legislation. This bill would have required data-collectors to provide consumers with information on the entity collecting the information and the purposes for which the information was being collected.

Furthermore, in 2005 I held two hearings on identity theft and security breaches involving personal information. These hearings led me to introduce the Data Accountability and Trust Act which would have required any entity that experiences a breach of security such as a business to notify all those in the United States whose information was acquired by an unauthorized person as a result of that breach.

So, Mr. Chairman, I look forward to our hearings. Protecting consumers' privacy is a very serious issue and one that needs to be fully examined and I think your leadership on this is to be commended and I look forward to continuing our work together.

Mr. BOUCHER. Well, thank you very much, Mr. Stearns, and let me simply briefly respond by saying that I appreciate and agree with your suggestions for the focus of our future hearing or hearings on this very important set of privacy concerns. And I want to acknowledge the gentleman's leadership in sponsoring comprehensive and thoughtful legislation in previous Congresses relating to privacy. I was pleased at that time to be the lead Democratic cosponsor of the gentleman's bill. And will be, well, I couldn't resist noting that, and we will be relying on the gentleman's experience and expertise on this subject as we construct bipartisan privacy legislation in this Congress.

The gentlelady from California, Ms. Eshoo, is recognized for 2 minutes.

OPENING STATEMENT OF HON. ANNA G. ESHOO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Ms. ESHOO. Thank you, Mr. Chairman, for holding this hearing on network privacy.

As a member of the House Intelligence Committee, I understand that the most valuable intelligence is to know how someone thinks because that enables one to predict what they might or will do in the future. Network operators want to monetize this predictability and profit from it. On its face, this is not an insidious practice. What is concerning is that the market is largely unregulated.

In the digital age we can aggregate enormous amounts of data, including what Web sites are viewed, search terms entered, programs viewed, items bought and sold, web applications utilized and other forms of data most of us don't even realize is being collected. With this information, a powerful profile can be created which can be used to target specific advertisements that are more relevant to the user.

We are here today to examine once again this growing issue. How do we regulate personal data collected by web companies and by network operators? Should we? And today we are obviously focusing on the network operators.

There is a growing tide of critics in this debate that I believe fundamentally do not understand the purpose of our privacy laws. These voices, some of them testifying today, believe that web-based services and telecommunications carriers should be subject to the same privacy regulations. I don't think this is practical or prudent. There is a fundamental difference between offering up free web-based advertiser supported applications and services, and a common carrier offering voice and broadband services. These separate and distinct services should each be governed fairly. That doesn't mean within the same regulatory structure. A healthcare provider and a stock broker shouldn't be regulated, in my view, under the same structure. Each should have its own. A consumer's relationship with their phone or broadband provider is not the same relationship they have with a search engine or an online vendor.

I am eager to hear from all of our witnesses. I am glad that you are all here today to hear about your practices and how you would envision privacy regulations. This is a very important debate and I hope that the final result will be a very sound and prudent bill that can be taken to the floor of the House.

So thank you, Mr. Chairman, for kicking off this series of hearings.

Mr. BOUCHER. Thank you very much, Ms. Eshoo.

The gentlelady from California, Ms. Bono Mack, is recognized for 2 minutes.

OPENING STATEMENT OF HON. MARY BONO MACK, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Ms. BONO MACK. Good morning, Chairman Boucher, Ranking Member Stearns and distinguished panel. Thank you for holding a hearing on the important issue of consumer privacy and broadband networks.

When a consumer makes a telephone call, purchases a good online, visits a Web site or watches a TV program on his couch, there is a built-in expectation of privacy associated with each activity. It is understood that our personal privacy is something of value. We have laws which protect privacy and the assurance of privacy is a marketable quality.

It is also important to note that cost of certain commercial activity on broadband networks is deflected away from the consumer because of advertising. As many of you know, I have a long history of working to protect consumers in the online space. In past Congresses I authored anti-spyware legislation and this is the second consecutive Congress I have introduced the Informed P2P User Act, therefore my legislative history speaks for itself. Additionally, I also have a history of fighting to prevent piracy online so I am willing to listen to efforts that reduce the impact piracy has on our national economy, as well.

As we begin the process of balancing consumer privacy and commercial activities online, I would like to listen to all sides of the debate and all parties involved in the online space. This includes consumers, law enforcement, ISPs, tech companies, search engines, advertisers, as well as content creators. It is my belief that both the privacy expectations and commercial activity need to be measured before we act. The committee would be wise to begin with the American consumers' privacy expectations in mind. I do not look at this issue as a partisan matter and I don't think we should be out to get one particular company or favor one particular industry. With that said, I do admit that sometimes a one size fits all approach is not possible in achieving certain goals. As such, I will be paying close attention to the debate and I look forward to working on this important issue.

Thank you, Mr. Chairman. I yield back.

Mr. BOUCHER. Thank you very much, Ms. Bono Mack.

The gentlelady from Colorado, Ms. DeGette, is recognized for 2 minutes.

Ms. DEGETTE. Thank you very much, Mr. Chairman. I want to thank you for having this important hearing today.

As technology changes and as consumer habits change, so do the privacy concerns that we are faced with and so I am looking forward to hearing from all of the witnesses today as we continue in our evolving discussion of privacy.

And with that, I will yield back.

Mr. BOUCHER. Thank you very much, Ms. DeGette. We will add 2 minutes to your time to question the panel of witnesses based upon that waiver.

The gentleman from California, Mr. Radanovich, is recognized for 2 minutes.

OPENING STATEMENT OF HON. GEORGE RADANOVICH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. RADANOVICH. Thank you, Chairman Boucher. I want to thank you and Mr. Stearns for holding this consumer privacy meeting and I do want to thank you, Mr. Chairman, I am pleased to hear that we will have a joint hearing on online advertising. It will be important for us to hear from the full technology landscape that utilizes private user information before we can move forward with any comprehensive effort to address this issue. I look forward to working with you on that hearing, as well.

One of the primary issues that has developed with communications and the Internet is the collection of consumer data. As technology advances and becomes more complex, consumers are rightfully concerned about their personal information. What we should focus on when it comes to consumer data is the consumers and what they care about and I believe that we should invoke looking at what data is collected, why it is collected and what is done with it. This information will help us all work together with the industry to achieve our goal of meeting the consumer needs by preventing the misuse of their information.

What I think that we should be looking at for most is the most effective way to protect our constituents' information in a manner that recognizes there are beneficial users for many of these new technologies and continues to allow for innovation that can make the communications experience more enjoyable, more productive and safer for us all.

I want to thank all of our witnesses for being here today and to discuss a wide variety of networks and their relationship to privacy. Your experience will certainly help us as we continue and I look forward to a productive hearing.

Thank you, Mr. Chairman.

Mr. BOUCHER. Thank you, Mr. Radanovich.

The gentleman from Michigan, Mr. Stupak, is recognized for 2 minutes.

OPENING STATEMENT OF HON. BART STUPAK, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. STUPAK. Thank you, Mr. Chairman, and thank you for holding this hearing.

It is time we modernized our telecommunications policies in regard to privacy. An individual's right to privacy has been under increasing assault as more Americans are using the Internet for more and more of their daily activities. Consumers do not have a clear picture of what occurs with their information without their consent and what needs to be done.

Last year this subcommittee held a hearing on a new type of data gathering for the purpose of behavioral advertising. This new method uses network technology known as deep pack inspection to read 100 percent of a web user's activities to create a profile for purposes of reselling it to advertisers. Companies that wish to utilize this technology have claimed that personally identifiable information is protected but I have my doubts and concerns.

As it stands right now, The Communication Act gives no clear definition of when affirmative consent or opt-in is required in the handling of a consumer's personal identifiable information. Without clear direction from Congress on this matter, technology will continue to outpace our privacy laws and consumer personal information will continue to go unprotected. Any method of collecting personally identifiable information from an Internet user's online activity for the purpose of reselling that information must require an opt-in from that user. In addition, that user should also be provided with the information on how and what is happening with their data, how it is collected and who is receiving it.

I look forward to hearing from our witnesses today on how we can modernize our privacy laws to protect, inform and empower consumers.

Thank you, Mr. Chairman, again for holding this hearing. I look forward to working with you and our colleagues to move legislation on this subject.

Mr. BOUCHER. Thank you very much, Mr. Stupak.

The gentlelady from Tennessee, Ms. Blackburn, is recognized for 2 minutes.

OPENING STATEMENT OF HON. MARSHA BLACKBURN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE

Ms. BLACKBURN. Thank you, Mr. Chairman. I want to thank you for holding the hearing today. And I want to welcome all of our witnesses and thank you for being here with us today.

Consumer privacy as you have heard from everyone who has spoken is a key element in the unspoken contract between the end user and the ISP and the merchants who make their living providing goods and services online. When any link in that chain of trust is broken, consumers at every level are going to suffer. It is therefore critical for Congress and our partners in the administration, the private sector and the consumer advocacy community to remain vigilant in securing consumer privacy online.

It is also critical on the other hand that Congress ensure vibrancy in the marketplace. And I think that is where many of us are going to have questions and want to explore a little bit more deeply with you to make certain that we have a good understanding of the deep packet inspection technologies and that we move forward in the appropriate way.

Mr. Chairman, I am pleased to know that we are going to do another hearing on the Google issues that are in front of us and I look forward to working with you on that hearing. And I hope that we can all send a message that piracy does not pay. That privacy and respect for intellectual property is an imperative and I look forward to the hearing.

I yield back.

Mr. BOUCHER. Thank you very much, Ms. Blackburn.

The gentlelady from Florida, Ms. Castor, is recognized for 2 minutes.

Ms. CASTOR. Thank you, Mr. Chairman, for this timely hearing on the evolution of our communications networks and consumer privacy. Welcome to our panel. I look forward to your expert advice

in learning a great deal more about this issue and I will yield back the remaining portion of my time.

Mr. BOUCHER. Thank you very much, Ms. Castor. We will add 2 minutes to your questioning time for the first panel.

The gentleman from Nebraska, Mr. Terry, is recognized for 2 minutes.

Mr. TERRY. Thank you, Mr. Chairman. I would waive and appreciate 2 minutes.

Mr. BOUCHER. You shall have the same.

[The prepared statement of Mr. Markey follows:]

Statement of
U.S. Representative Edward J. Markey (D-MA)
Hearing on Electronic Privacy
April 23, 2009

Good Morning. I want to commend Chairman Boucher for holding this hearing on electronic privacy issues.

Many of the issues the Subcommittee will explore this morning are issues that the Subcommittee has touched on before, particularly the issues surrounding deep packet inspection. Privacy however in the digital environment must reflect the myriad ways in which consumers now interact with technology and applications. We have provisions to protect consumer privacy related to cable operators for all communications-related services that utilize cable facilities, on traditional telephone companies, and on wireless service providers. This is an opportune moment to revisit these provisions to ensure their adequacy and gauge whether clarifications of provisions or the harmonization of obligations across providers and platforms is warranted to reflect convergence and the advent of new applications and services.

For instance, I successfully offered the amendment in this Subcommittee 10 years ago to ensure that wireless providers that implemented location technology and disclosed it during emergencies, did not utilize the same technology to gather location information about users or disclose it without the “prior express authorization” of the subscriber. Now that our wireless policies are yielding success to the extent 3^d party application providers—and not just the wireless carriers themselves – can offer such location services, I believe such application providers ought to have the same legal privacy obligations that wireless carriers do today.

When I sponsored and successfully passed the Children's Online Privacy Protection Act it was well before the current rise in behavioral advertising and targeting. I believe we should revisit the need to protect children from such business practices.

There will undoubtedly be many compelling services and applications that will rely upon advertising as part of their business model. I am not interested in banning all advertising or marketing models. I do believe, however, that consumer privacy principles are immutable and technologies and services should be animated by these principles rather than effectively undermining them. Any practices that surreptitiously gather personal information, or unreasonably retain such data, or fail to adequately and meaningfully disclose important data security and data use practices to consumers, or fail to extend to consumers the right to effectively control such collection and subsequent use, are operating on the edges of ethical conduct and straying from long-held privacy principles.

This is a timely hearing. My Chairman, I understand that you and Chairman Rush are planning a joint hearing of this Subcommittee and the Subcommittee on Commerce, Trade and Consumer Protection that will include witnesses from web-based services and applications so that we more adequately cover the telecommunications terrain that consumers traverse with their personal data every day. I support such an approach because, ultimately, I support legislating in a comprehensive fashion in this area and look forward to working with Chairman Boucher, Ranking Member Stearns, Chairman Waxman, Ranking Member Barton, and other Committee colleagues on these important consumer issues in the months ahead.

Thank you.

Mr. BOUCHER. All members having now been recognized for opening statements, we turn to our panel of witnesses and express appreciation to each of you for your testimony here this morning. Ms. Leslie Harris is the president and chief executive officer of the Center for Democracy and Technology. Mr. Kyle McSillarow is president and chief executive officer of the National Cable and Telecommunications Association. Mr. Marc Rotenberg is the executive director of the Electronic Privacy Information Center. Ms. Dorothy Attwood is chief privacy officer for AT&T Services. Mr. Ben Scott is policy director for Free Press. Mr. Brian Knapp is chief operating officer of Loopt. And Mr. Richard Bennett is a network engineer and a blogger and we welcome each of you. Without objection, your prepared written statements will be made part of the record. We would ask for your oral summary be kept to approximately 5 minutes so that we will have ample time for questions.

And, Ms. Harris, we are pleased to begin with you and you need to turn your mike on. It is amazing how many people in the technology subcommittee don't have their mike on when they start to testify.

STATEMENTS OF LESLIE HARRIS, PRESIDENT, CHIEF EXECUTIVE OFFICER, CENTER FOR DEMOCRACY AND TECHNOLOGY; KYLE MCSLARROW, PRESIDENT AND CEO, NATIONAL CABLE AND TELECOMMUNICATIONS ASSOCIATION; MARC ROTENBERG, PRESIDENT AND EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER; DOROTHY ATTWOOD, SENIOR VICE PRESIDENT, PUBLIC POLICY AND CHIEF PRIVACY OFFICER, AT&T SERVICES, INC.; BEN SCOTT, POLICY DIRECTOR, FREE PRESS; BRIAN R. KNAPP, CHIEF OPERATING OFFICER, LOOPT, INC.; AND RICHARD BENNETT, PUBLISHER, BROADBANDPOLITICS.COM

STATEMENT OF LESLIE HARRIS

Ms. HARRIS. Mr. Chairman, Mr. Stearns, members of the subcommittee, I appreciate the opportunity to testify on this important question of the privacy implications of DPI.

In CDT's view, DPI poses very serious challenges both to the privacy and to the openness of the Internet. The success of the Internet can be traced to its defining end-to-end principle which is a simple idea that applications are better left to be implemented at the edges of a network and leave the core unfettered by gatekeepers.

The end-to-end principle, as you know, is supported by a policy framework that generally protects Internet service providers for liability for the content that they are either posting or flowing over their networks. And together these two policy choices have really preserved the Internet as a trusted, open platform.

Today massive growth in data processing power has spurred the development of DPI and potentially allowing Internet service providers and other intermediaries and partners to analyze all of the Internet traffic of millions of users simultaneously. This raises profound questions about the future of privacy, openness and innovation online. Though deployment is still somewhat limited, applica-

tions range from management of congestion on the networks and network threats, content blocking, behavioral advertising and government surveillance.

It is my understanding that right now network operators are only using the technology for security-related purposes although, of course, last summer we did have a failed attempt to use it for behavioral advertising. Of course, some of these applications may have other troubling legal policy concerns but it is important to stress that all applications of DPI raise serious privacy concerns because all applications of DPI begin with the interception and analysis of traffic.

In our view, deep packet inspection is really no different than postal employees opening envelopes, reading letters inside. DPI networks intercept and examine the entire payload of a packet, the actual data that the packet carries in addition to a packet header unless the content is encrypted.

So even if ISP's or advertising networks intend to only use a small portion of what is captured by DPI and dispose of the rest, it doesn't diminish the breadth and intrusiveness of that initial data capture. And DPI is being deployed within a technological environment where consumers are sending more and more information through the networks. Providers of all kinds are acquiring and collecting and holding more data and sharing it and it is being retained for longer periods of time and all of this without an adequate legal framework.

Consumers simply do not expect to be snooped on by their ISPs or other intermediaries in the middle of the network. And so therefore DPI really defies the legitimate expectations of privacy that consumers have and it is also at odds with fair information practices, concepts like transparency, concepts like limited collection of data. The sectoral privacy laws that we have, have been far outpaced by technological innovation and as many of you have said, we have no baseline consumer privacy law.

Finally, as DPI matures and becomes more widely deployed, our concern is that any notion of limited use is going to give way to mission creep as new applications are deployed. And that mission creep, frankly, is not just a concern that the providers will find new ways but that government and policymakers will increasingly have mandates to networks to use DPI for various purposes. And, of course, we worry as well about the sort of unlimited appetite for surveillance that our government appears to have and the fact that DPI really is a game changer there as well.

For all these reasons, we applaud the fact you are taking a comprehensive look at DPI. We obviously think that, you know, the most important thing that can happen this year is an acting baseline, technology neutral consumer privacy legislation based on fair information practices. We are very pleased to hear the announcement, Mr. Chairman, and the support from the committee. I will just say that we also hope the subcommittee might move ahead with carefully crafted Internet neutrality legislation because we think it might put some balance on the more worrisome uses of DPI. And finally, it is outside of your jurisdiction, I think, but Congress has to examine and strengthen the communications privacy laws, ECPA, et cetera, at the same time which has to do with gov-

ernment access because all of these have been outstripped by technology and really change the nature of what privacy protections really exist at this point for consumers.

So thank you so much.

[The prepared statement of Ms. Harris follows:]

Statement of Leslie Harris
 President and Chief Executive Officer
 Center for Democracy & Technology

Before the House Committee on Energy and Commerce,
 Subcommittee on Communications, Technology and the Internet

“The Privacy Implications of Deep Packet Inspection”

April 23, 2009

Chairman Boucher and Members of the Subcommittee:

On behalf of the Center for Democracy & Technology (CDT), I thank you for the opportunity to testify today. We applaud the Subcommittee’s leadership and foresight in examining the privacy implications of the technique known as “deep packet inspection” (DPI).

In CDT’s view, DPI poses serious challenges both to privacy and to the openness and innovation that are the hallmarks of the Internet. The success of the Internet can be traced in part to its defining “end-to-end” principle: the simple idea that applications are better left to be implemented at the Internet’s endpoints rather than its core, leaving the network itself unfettered by any particular party’s interests.¹ Pursuant to this end-to-end design, data has traditionally traversed the Internet without interference from gatekeepers.

The end-to-end principle is supported by a policy framework that generally protects Internet service providers from intermediary liability (i.e., liability for content that originates with users) unless the network operator is directly involved in the creation of the content.² For decades, adherence to the end-to-

¹ J.H. Saltzer, D.P. Reed & D.D. Clark, End-to-End Arguments in System Design, 2 ACM Transactions on Computer Sys. 277 (1984).

² As part of the Telecommunication Act of 1996, Congress enacted broad immunity for ISPs and online service providers from liability for content posted by customers or third parties. See 47 U.S.C. § 230. Section 230 has been a critical foundation for the huge explosion of “Web 2.0” content and services on the Internet. For information on the origin and scope of Section 230, see an amicus brief that CDT filed with the 9th Circuit in 2008, available at www.cdt.org/privacy/spyware/20080505amicus.pdf.

end principle has preserved the Internet as a trusted platform and has supported unparalleled levels of innovation, economic activity, and individual expression.

In recent years, however, massive growth in data processing power has spurred the development of new “deep packet inspection” (DPI) technologies that potentially allow Internet service providers (ISPs) and other intermediaries to analyze all of the Internet traffic of millions of users simultaneously. The use of DPI technology, though still in somewhat limited deployment, raises profound questions about the future of privacy, openness, and innovation online.³

It is important to stress at the outset that *all* applications of DPI raise serious privacy concerns because all applications of DPI begin with the interception and analysis of Internet traffic. Policymakers must carefully consider each use of DPI and balance the perceived benefit of its use against the risks to privacy and civil liberties, as well as to the Internet’s character as an open platform. CDT believes that only rare uses of DPI will be acceptable after such a balancing. Today, DPI applications include management of network congestion, detection of network threats, content blocking for intellectual property protection and child safety, behavioral advertising, and government surveillance.

CDT has been outspoken in opposition to government-mandated content filtering by ISPs⁴ and in support of the call for Internet neutrality legislation to prohibit discrimination between Internet data streams.⁵ While we will briefly discuss those issues below, our testimony today will principally focus on the privacy implications of DPI. This statement builds on testimony we gave to this Subcommittee last July,⁶ taking into account developments since then.

Unlike other media, the Internet is decentralized. Control is vested at the ends of the network with its individual uses, and its end-to-end communications are largely unfettered. Consumers expect that their Internet transmissions will not be intercepted or analyzed en route by an intermediary. DPI systems defy this

³ Packet inspection or data analysis that a user conducts on his or her own data stream is a different matter and does not raise the same questions. There are many reasons why a user may want to conduct such analysis, and the ability to do so empowers users to better understand their own Internet usage or service plans. This testimony focuses exclusively on packet inspection and analysis by intermediaries at the middle of the network rather than at the endpoints.

⁴ See, e.g., CDT, Summary and Highlights of the Philadelphia District Court’s Decision in *Center for Democracy & Technology v. Pappert* (Case No. 03-5051 (E.D. Pa. Sept. 15, 2004)), <http://www.cdt.org/speech/pennwebwebblock/20040915highlights.pdf>.

⁵ See CDT, *PRESERVING THE ESSENTIAL INTERNET* (2006), <http://cdt.org/speech/20060620neutrality.pdf>. More recently, we recommended to the Federal Communications Commission that ISPs’ endeavors to manage congestion on their networks – which may include the use of DPI – be transparent, evenly applied to all services and applications, and consistent with core internetworking standards. See Comments of CDT, *In the Matter of Broadband Industry Practices*, WC Docket No. 07-52 (Feb. 13, 2008), http://cdt.org/speech/20080213_FCC_comments.pdf.

⁶ Alissa Cooper, Testimony of Alissa Cooper before the House Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet: “*What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies*” (July 17, 2008), <http://cdt.org/testimony/20080717cooper.pdf>.

expectation, threatening the basis for consumer trust online. The use of DPI is also at odds with well accepted “Fair Information Practices,”⁷ can be disruptive to Internet and Web functionality,⁸ and may – in some instances – run afoul of existing communications privacy laws.⁹

Companies that use DPI to track consumers’ online activities to serve targeted advertisements or to manage network congestion often stress the anonymous and limited nature of the information they compile. However, the privacy concerns that arise from the use of DPI begin with the interception, diversion or copying of substantially all of the Internet traffic of all subscribers. Just because ISPs or advertising networks may use only a small portion of what is captured and do not retain other information does not diminish the breadth and intrusiveness of the initial data capture.

DPI technologies are being deployed within a technological environment where consumers are sending more personal data through their ISPs than ever before, and more data is being collected, retained for longer periods, and shared among more parties. However, even while existing sectoral privacy protections have been far outpaced by technological innovation, our nation still has no baseline consumer privacy law. Self-regulation, while important, has proven to be insufficient to protect privacy in the online context. For all of these reasons, Congress needs to take a comprehensive look at the current and emerging practices associated with DPI, and should approach the technology with great skepticism. Congress should also take a comprehensive look at online privacy issues at large. We recommend that Congress take the following steps:

- Building on the inquiries posed last year by Chairman Markey,¹⁰ the Subcommittee should seek additional information directly from ISPs and their partners about how they are using DPI. Specifically, for what purposes are ISPs currently using DPI? Are additional uses anticipated? What information are ISPs collecting or examining, and how long is that information retained? Are ISPs using DPI on a continuous basis or only intermittently, such as in response to security incidents or to sample traffic for aggregate usage analysis? Are third parties paying ISPs to use

⁷ The FIPs are a set of generally accepted principles for protecting the privacy of personal data in a variety of contexts. The FIPs have become a standard model for privacy protection frameworks. See, e.g., Organisation for Economic Co-operation and Development, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (Sept. 23, 1980), http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

⁸ Richard Clayton, The Phorm “Webwise” System (May 2008), <http://www.d.cam.ac.uk/~rnc1/080518-phorm.pdf>.

⁹ See *An Overview of the Federal Wiretap Act, Electronic Communications Privacy Act, and State Two-Party Consent Laws of Relevance to the NebuAd System and Other Uses of Internet Traffic Content from ISPs for Behavioral Advertising*, Appendix A to the Statement of Alissa Cooper Before the Subcommittee on Telecommunications and the Internet of the House Committee on Energy and Commerce, 110th Cong. (2008), <http://cdt.org/testimony/20080717cooper.pdf>.

¹⁰ See Congressman Ed Markey, *Lawmakers Ask Top Broadband and Internet Co.s to Detail Use of User-Tracking Tech*, Aug. 1, 2008, http://markey.house.gov/index.php?option=com_content&task=view&id=3425&Itemid=141.

DPI to identify or manipulate or divert certain content? If so, for what purposes? In what circumstance – if any – have ISPs obtained the consent of their customers to conduct DPI? How has consent been obtained? In what circumstances do ISPs believe consent is not required?

- Based on its ongoing research into DPI and other critical privacy concerns, the Subcommittee should take the lead in developing baseline, technology-neutral consumer privacy legislation, based on Fair Information Practices, that will address not only DPI but also the range of privacy issues facing companies and consumers. Such legislation could limit the use of DPI and provide safeguards for its deployment in those cases where it is acceptable.
- Congress should work to enact Internet neutrality legislation that specifically addresses content discrimination by Internet service providers. This legislation should avoid overly detailed rulemakings or specific technical mandates and should respect ISPs' needs to secure their networks and manage congestion, while ensuring that discriminatory practices are not allowed to create new Internet gatekeepers and erode the medium's openness to innovation.
- Congress should examine and strengthen the communications privacy laws regarding government surveillance to cover new services, technologies and business models with consistent rules. In particular, the Electronic Communications Privacy Act (ECPA) needs to be revised to better reflect modern uses of digital communications technology. While that effort must be broader than DPI, and will probably fall under the jurisdiction of another Committee, the effort may benefit from the record created here.

Understanding Deep Packet Inspection

The easiest way to understand deep packet inspection is to consider an analogy to the postal mail system. In the postal system, letters travel through the system in envelopes, each of which is addressed to its appropriate recipient and contains the return address information of the sender. On the Internet, data is broken into "packets." This is true for all kinds of Internet communications: Web browsing, email, voice-over-IP (VoIP) phone calls, peer-to-peer (p2p) file transfers, online gaming and so on. A single packet consist of two parts: a "payload," which is the actual data inside the packet, like the letter inside an envelope; and a "header," which contains the routing information that directs

the packet to its destination (or back to the sender in case of errors), like the address and return address on the outside of an envelope. For an Internet packet, the IP addresses of the recipient and sender, respectively, are equivalent to the address and return address on an envelope in the mail.

As postal employees and equipment move mail through the system, they inspect the addressing information on the outside of each envelope to determine the next step in directing the mail to its final destination. The same is true for the Internet – the devices in the middle of the network responsible for routing data (known as “routers”) inspect packet headers to decide where each packet should go next. This is called “shallow packet inspection” because the analysis is limited to the header information that is automatically exposed (by necessity) to every router on the Internet. Just as the postal mail simply cannot be delivered without postal employees and equipment inspecting addresses, neither can Internet communications be delivered without routers inspecting packet headers. However, this shallow sort of inspection does not reveal the actual content of the Web browsing session, email, or VoIP call that a particular packet may contain, just as looking at an address on an envelope reveals nothing about the content of the letter inside.

Deep packet inspection is the equivalent of postal employees opening envelopes and reading the letters inside. To do DPI, network devices examine the payload of a packet – the actual data the packet carries – in addition to the packet header. To inspect a packet deeply means to examine the contents of the Web browsing session, email, instant message, or whatever other data the packet contains. Unless the content of the packet is encrypted (as with most online purchases and bank transactions), the entirety of the packet can be analyzed with DPI.

One slight complexity of Internet packets is that a packet payload itself may contain some additional addressing information that is supplemental to the IP addresses available in the packet header. When sending an email, for example, the email address of the recipient appears in the packet payload, not in the packet header. Likewise for Web browsing, the name of the Web site that a user is trying to reach appears in the payload, not the header. These kinds of additional addressing information are sometimes referred to as “application headers” because they are specific to particular Internet applications (Web browsing, email, or VoIP, for example).

Although some may claim that examining such application headers does not constitute deep packet inspection,¹¹ CDT disagrees. Application headers have

¹¹ See, e.g., Declan McCullagh, *Q&A with Charter VP: Your Web activity, logged and loaded*, C1Net, May 15, 2008, http://news.cnet.com/8301-13578_3-9945309-38.html.

the potential to reveal much more about a communication than packet headers, and the task of determining where an application header stops and actual data content begins often necessitates the inspection of the data content itself. Therefore, we believe the line between shallow and deep inspection lies between the packet header and the packet payload, regardless of whether the payload contains these additional “application headers.”

DPI may be done in real-time as the data is in transmission, or it may be done afterward if the data is retained. ISPs may house DPI equipment and conduct the packet inspection themselves, or they may allow a third party intermediary to attach equipment to collect and inspect the Internet transmissions of their subscribers.

The Privacy Risks of Deep Packet Inspection

CDT believes that DPI in nearly every context raises substantial privacy concerns. In part because the Internet was developed around the end-to-end principle, consumers have come to expect that their Internet communications pass through the network without being snooped on along the way. DPI dramatically alters this landscape by providing an ISP or its partners with the ability to inspect consumer communications en route. Thus, deploying a DPI system defies the expectations consumers have built up over time. Absent unmistakable notice, consumers simply do not expect their ISP or its partners to be looking into the content of their Internet communications.

Many companies at every level of the Internet have worked to build trust in the medium to the point where millions of consumers feel comfortable engaging in a wide range of personal and commercial communications and transactions online. ISPs are a critical part of that chain of trust. If consumers find reasons to question what their ISPs are doing with their Internet data, DPI runs the risk of damaging consumer confidence in the medium.

Certain characteristics of DPI also seriously challenge traditional Fair Information Practices. Consider the FIPs principle of limiting data collection to what is necessary to complete the task at hand. How can this idea be squared with DPI equipment that has the capability to collect and analyze every single Internet packet for millions of Internet users?¹² Although DPI can be implemented with limits on the types of data collected, the legal framework

¹² See ProCera, PacketLogic PL10000 Series, <http://www.proceranetworks.com/images/datasheets-2008-11-03/DS-PL10000-11-3-08.pdf> (last visited Apr. 19, 2009).

provides almost no useful guidance for where such limits should be set, given the lack of a comprehensive privacy law in the U.S.

Transparency is another core FIPs principle that DPI challenges. DPI equipment vendors compete on how invisible an impact their technology will have on overall network operations.¹³ Vendors seek to ensure that DPI equipment, even as it processes masses of Internet data from millions of subscribers, will not slow down network operations and will in fact be almost entirely undetectable. This means ISPs and others may be able to deploy DPI systems that are invisible even to sophisticated consumers. With DPI hidden from view, consumers will be largely unaware that their data streams are being intercepted and thus those doing the packet inspection may have little incentive to fully disclose their practices.

In many cases, DPI equipment will automatically collect personally identifiable information (PII), even if the ISP or its partners have no intentions of using such data. Consider a third-party vendor using a DPI system to analyze the Web browsing activities of an ISP's subscribers. Although the vendor may not care to know the home address of a subscriber, the DPI equipment surely intercepts and collects PII when that subscriber conducts Web searches to obtain online driving directions from his or her own home address. Furthermore, DPI systems automatically collect IP addresses, which can sometimes be used to re-identify individuals when combined with other information. In this way, DPI tends to sweep in personal information even when the party doing the packet inspection does not seek such information.

Similarly, sensitive information may be unintentionally collected in a DPI system. Personal health data, for example, is migrating online through an ever-expanding array of health information and search sites, online support groups, and personal health record sites. Although the operator of a DPI system may not care to store or analyze such information, a packet containing sensitive data must first be inspected to determine its contents before the DPI system operator can decide what to do with it. In short, DPI technology may look at all information, including sensitive information; what is then done with that information can vary widely and is unlikely to be directly observable by consumers.

Finally, as DPI technology matures and becomes more widely deployed, it will also pose serious threats in terms of government surveillance. As a general

¹³ See, e.g., The Tolly Group, ProCera PacketLogic 7600 Evaluation of Accuracy and Scalability of Network Traffic and Service Management System (May 2007), <http://www.proceranetworks.com/images/documents/tolly207173procerapacketlogic7600may2007.pdf> (highlighting the fact that the ProCera DPI device "generates less than 1 millisecond of one-way average latency").

matter, the rules for government surveillance have failed to provide adequate privacy protection in the face of technological change. The implications of DPI remain largely unexplored, although the government has clearly displayed a seemingly unlimited appetite for electronic surveillance. For criminal investigations, government monitoring of the content of communications is still limited by the principles of probable cause and particularity, but the rules for monitoring of transactional data are very weak.

In the context of national security, the 2008 changes to the Foreign Intelligence Surveillance Act may have permitted bulk collection of both transactional data and the content of international communications. Last week's revelation in the New York Times of significant "over collection" illustrates the risks of permitting government surveillance without adequate judicial checks and balances.¹⁴ The problem is that the government can use any capability deployed for commercial purposes. Widespread deployment of DPI, whether or not it is initially used for legitimate commercial purposes, would offer to the government a staggering ability to closely and constantly monitor Internet communications. It is probably fair to say that there are not in place today adequate rules of judicial approval and oversight to control the use of that capability.

In sum, DPI poses unique risks to individual privacy. Moreover, once the technology is acquired for a legitimate purpose such as responding to network threats, it will be hard to draw the line at ever more intrusive uses as third parties approach the network operators with proposals to monetize Internet traffic and the government makes greater demands. Given DPI's intrusive nature, this Subcommittee is right to closely examine its current and projected uses and consider its risks.

■ Concerns in Addition to Privacy

In addition to the foregoing privacy concerns, which CDT believes are implicated by all uses of DPI, the practice can raise a number of other concerns which will vary by specific application. While the focus of this testimony is on the broad privacy consequences of DPI, this section will briefly address some additional concerns which merit serious consideration as Congress continues its investigation of DPI.

¹⁴ Eric Lichtblau and James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, New York Times April 15, 2009, <http://www.nytimes.com/2009/04/16/us/16nsa.html>.

Using DPI to identify specific types of communications for the purposes of prioritization – for example, in response to network congestion or pursuant to ISP partnerships with content providers – can undermine the openness of the Internet and threaten its status as a platform for innovation. Historically, open and standardized technical protocols have enabled innovators to develop and deploy new content and services on the Internet without needing to seek permission from any gatekeeper. DPI could place the power to discriminate among content and services in the hands of network-level intermediaries, threatening this openness and hindering future innovation. CDT believes that network providers should not be in the business of picking winners and losers from among Internet content and services,¹⁵ and some uses of DPI could increase the risk that this could happen.

Using DPI to identify and filter or block certain illegal or undesirable content, for such diverse purposes as child protection or copyright enforcement, would raise additional concerns. Content filters can suffer from overbreadth problems, blocking material beyond that for which they are intended, including constitutionally protected material.¹⁶ Filters designed for copyright enforcement may fail to account for fair use and the possibility that a particular Internet user might be authorized to make a particular intercepted transfer. Perhaps most importantly from a policy perspective, broad use of DPI to detect and block illegal or undesirable content on the network could undermine U.S. advocacy for Internet freedom in repressive regimes around the world. As one example, the Chinese government has already deployed DPI filtering to censor material it finds objectionable from the Internet.¹⁷ U.S. efforts to press foreign regimes to abandon Internet surveillance and censorship may be undercut if we are seen to engage in similar behavior with respect to our own designated classes of forbidden content.

■ Assessing Potential Uses of Deep Packet Inspection

In assessing specific uses of DPI, the first thing to note is that some may already be regulated or prohibited under the federal Wiretap Act and the Cable Act. In a memo issued last July, CDT explored in some depth the application of the

¹⁵ CDT has proposed a framework for Internet neutrality legislation that specifically addresses the issue of content discrimination by ISPs. See CDT, Transition Memo for President Barack Obama: Internet Neutrality, November 2008, available at <http://cdt.org/transition/InternetNeutrality.pdf>.

¹⁶ See *supra* note 4.

¹⁷ Richard Clayton, Stephen J. Murdoch, and Robert N. M. Watson, *Ignoring the Great Firewall of China*, presented at 6th Workshop on Privacy Enhancing Technologies, Robinson College, Cambridge, United Kingdom (June – June 30, 2006), <http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf>.

Wiretap Act and related laws to DPI.¹⁸ We concluded that certain uses of DPI to compile behavioral advertising profiles would probably run afoul of the Wiretap Act absent unavoidable notice and “opt-in” consent. Last September, without expressly embracing our legal analysis, AT&T, Verizon, and Time Warner Cable committed to providing notice and obtaining affirmative consent from consumers before tracking their Web activity for targeted online advertising.¹⁹ However, the boundaries of the Wiretap Act are not clear in all contexts. Moreover, the Act was last modified more than 20 years ago and has not kept pace with technology. It simply does not provide sufficient protection to consumers against DPI’s risks.

Also, consent has its limitations. For example, it is still difficult to see whether and how unavoidable notice and true consent can be provided in settings where there is little regular communications between the ISP and the customer. Consent is further complicated in the residential context or any other situation where more than one person uses a single Internet connection.²⁰ As a general matter, online providers have not yet provided an opt-out mechanism in the advertising context that the majority of consumers can effectively utilize, and applications of DPI for behavioral advertising would seem to suffer from the same limitations. Opt-out mechanisms for online advertising are often buried in fine print, difficult to understand, hard to execute and technically inadequate. Only the most sophisticated and technically savvy consumers are likely to successfully negotiate such opt-out processes. Moreover, while a robust notice and opt-in regime might mitigate some privacy concerns of DPI for behavioral advertising, consumers may lack an incentive and are therefore highly unlikely to opt-in to the use of DPI for content filtering or congestion management.

Looking beyond the limitations of consent and the current legal framework, ISPs and policymakers should approach DPI with great skepticism. They should carefully weigh any expected benefits of a proposed use of DPI against the substantial privacy and other risks outlined above. They also should consider whether there may be alternative methods for achieving their goals, with a strong preference for means that do not require sweeping inspection of Internet communications at the ISP level.

¹⁸ See *An Overview of the Federal Wiretap Act, Electronic Communications Privacy Act, and State Two-Party Consent Laws of Relevance to the NebuAd System and Other Uses of Internet Traffic Content from ISPs for Behavioral Advertising*, Appendix A to the Statement of Alissa Cooper Before the Subcommittee on Telecommunications and the Internet of the House Committee on Energy and Commerce, 110th Cong. (2008) <http://cdt.org/testimony/20080717cooper.pdf>.

¹⁹ See *Broadband Providers and Consumer Privacy*, Hearing before the Senate Committee on Commerce, Science and Transportation, September 25, 2008 http://commerce.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=778594fe-a171-4906-a585-15f19e2d602a.

²⁰ Paul Ohm, *The Rise and Fall of invasive ISP Surveillance*, University of Illinois L. Rev (2009), Pgs. 62-65, <http://ssrn.com/abstract=1261344>.

In terms of alternatives to DPI that do not raise the same concerns, network management offers a good example. It has been proposed that an ISP could use DPI to help manage network congestion, by peering into the content of subscribers' traffic to try to identify which traffic appears to need delivery priority and which does not. But alternative congestion management techniques could serve the same goals without inspecting any packet payloads.²¹ A congestion management tool that focuses on addressing high volume users responsible for the majority of network traffic does not require DPI because it is content-agnostic. It needs to know the overall volume of bandwidth each user is consuming, but does not care what the content is.

Another proposed tool for DPI is to identify network threats such as spam, malware, and denial-of-service attacks. There may be instances where this would be the most effective and efficient technique. There are also, however, a variety of other security tools available, including tools that operate at the endpoints of the network. Spam filters and anti-malware software, for example, can be deployed at the application level by individual computer users (on email servers, for example), on Web servers, and so forth. There is also a big difference between using DPI sporadically, in response to a current threat or attack, and employing it on an ongoing basis. Security techniques based on DPI should be employed only in targeted fashion when they are truly superior to available alternatives.

DPI aimed at reducing online copyright infringement is likewise just one of a number of possible anti-infringement tools. Other means include lawsuits against infringers and the DMCA's notice-and-takedown regime. Just as important, there are steps that can and are being employed at the edges of the network. Individual websites and content hosting services, such as YouTube and MySpace, actively employ filters to identify copyright-infringing material.²² Such filtering raises a variety of policy questions, but it does not involve ISP-level DPI and hence does not raise the same level of privacy concerns.

In short, ISPs and policymakers assessing a proposed use of DPI need to consider whether the practice is legal, whether the benefits would really outweigh the substantial costs and whether there are preferable alternatives. CDT believes strongly that this analysis will rarely favor the use of DPI on a broad scale.

²¹ See, e.g., Filing of Comcast, Inc., *In the Matter of Broadband Industry Practices*, WC Docket No. 07-52 (September 19, 2008), http://hja.licensing.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6520169715.

²² See, e.g., YouTube.com, "Audio ID and Video ID," <http://www.youtube.com/t/contentid>.

The Privacy of Location Information

The Subcommittee has also expressed interest in privacy issues relating to location information. Although disclosure of location information can sometimes involve deep packet inspection, such disclosure more commonly happens through a location-based service or application without DPI. However, CDT strongly shares the Committee's concern about the privacy of location information.

The ubiquity of increasingly high-powered mobile devices has already spawned the Internet's first generation of location-based services and applications. As the accuracy of location data improves and the expense of calculating and obtaining it declines, location may well come to pervade the online experience. While the increasing availability of location information paves the way for exciting new applications and services, the increasingly easy availability of location information raises several different kinds of privacy concerns. Ensuring that location information is transmitted and accessed in a privacy-protective way is essential to the future success of location-based applications and services.

Because individuals often carry their mobile devices with them, location data may be collected everywhere and at any time, often without user interaction, and it may potentially describe both what a person is doing and where he or she is doing it. For example, triangulation of an individual's mobile phone can reveal the fact that he was at a particular medical clinic at a particular time. The ubiquity of location information may also increase the risks of stalking and domestic violence if perpetrators are able to use (or abuse) location-based services to gain access to location information about their victims.

Furthermore, location information is and will continue to be of particular interest to governments and law enforcers around the world. Standards for government access to location information held by companies are unclear at best and far too low at worst.²³ The existence of detailed records of individuals' movements should not automatically facilitate the ability for governments to track their citizens, but in many cases, laws dictating what government agents must do to obtain location data have not kept pace with technological evolution.

²³ See Center for Democracy & Technology, "Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology" (2006), available at <http://www.cdt.org/publications/digital-search-and-seizure.pdf>. Over the past few years courts have split on the standards protecting location information, with a majority of courts rejecting governmental arguments for a low standard. See, e.g., *In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communications Service to Disclose Records to the Government*, No. 07-524M (W.D. Pa. Sept. 10, 2008), (available at <http://www.eff.org/files/filenode/celltracking/lenihanorder.pdf>). CDT joined an amicus brief that details the key legal argument for a strong standards, available at http://www.cdt.org/security/20080731_lenihan_amicus.pdf.

Location-based services can be built to protect against privacy risks by, for example, obtaining affirmative user consent, strictly limiting how long location data is retained, and allowing users to set the precision of their location information. But the comprehensive and sensitive nature of location information collection demands that location-based services be deployed with such heightened protections in place.

CDT believes that there are at least three specific measures needed to protect the privacy of location information, the first two of which would benefit from Congressional action:

- First, the disclosure of precise location information in a commercial context must only be made with specific, informed, opt-in consent in which a user has the ability to selectively disclose location only to trusted parties.²⁴ As Congress contemplates enacting baseline consumer privacy legislation, such a requirement could easily be part of a broader framework governing sensitive consumer data.
- Second, the standards for government and law enforcement access to location information must be amended to make clear that a probable cause warrant is required for the government to obtain location information.
- Third, location-based services and applications should follow technical standards that give users clear control over the use of their location information and that require the transmittal of privacy rules with the location information itself.²⁵

As the Committee is aware, location information is particularly sensitive, and location-aware applications are increasingly pervasive. We look forward to working with the Committee to address the privacy concerns raised by the increasing availability of location information.

²⁴ Some of the location-based social networks and services have been very cautious about privacy, while unfortunately, some companies are seeking to distribute location with little or no privacy protections.

²⁵ CDT has worked since 2001 within the Internet Engineering Task Force (IETF) on the development of a location privacy standard named Geopriv. See Geopriv Working Group Charter, <http://www.ietf.org/html.charters/geopriv-charter.html>. For more information about this standard, see John Morris and Jon Peterson, *Who's Watching You Now?*, IEEE Security and Privacy Magazine, Vol. 5, Issue 1 (January/February 2007) (available at <http://www.cdt.org/publications/20070100ieee.pdf>). See also Alissa Cooper and John Morris, *Binding Privacy Rules to Location on the Web*, Proceedings of the 2nd International Workshop on Location and the Web, LOCWEB '09 (Boston, Mass., Apr. 04, 2009) (available at <http://www.cdt.org/privacy/LocWebFinal.pdf>).

The Role of Congress

Congress should take action to address the significant privacy concerns raised by DPI and broader online privacy issues:

- As a first step, following up on the inquiries made last year, we urge the Subcommittee to seek and compile for the public record additional information directly from ISPs and their partners about how they are using DPI. Specifically, for what purposes are ISPs currently using DPI? Are additional uses anticipated? What information are ISPs collecting or examining, and how long is that information retained? Are ISPs using DPI on a continuous basis or only intermittently, such as in response to security incidents or to sample traffic for aggregate usage analysis? Are third parties paying ISPs to use DPI to identify or manipulate or divert certain content? If so, for what purposes? In what circumstance – if any – have ISPs obtained the consent of their customers to conduct DPI? How has consent been obtained? In what circumstances do ISPs believe consent is not required?
- This Subcommittee should set a goal of enacting within the next year general privacy legislation covering both the online and offline worlds. CDT has long argued for simple, flexible baseline consumer privacy legislation that would protect consumers from inappropriate collection and misuse of their personal information while enabling legitimate business use to promote economic and social value. In principle, such legislation would codify the fundamentals of Fair Information Practices, including requiring transparency and notice of data collection practices, minimizing data collection and retention, providing consumers with meaningful choice regarding the use and disclosure of that information, allowing consumers reasonable access to personal information they have provided, providing remedies for misuse or unauthorized access, and setting standards to limit data collection and ensure data security. Although we believe communications privacy laws already apply to some applications of DPI, enacting baseline privacy legislation would further clarify consumers' privacy rights and create protections for other forms of data collection not covered under current law.
- Congress should work to enact Internet neutrality legislation that specifically addresses content discrimination by Internet service providers. This legislation should avoid overly detailed rulemakings or specific technical mandates and should respect ISPs' needs to secure their networks and manage congestion, while ensuring that

C E N T E R F O R D E M O C R A C Y & T E C H N O L O G Y

discriminatory practices are not allowed create new Internet gatekeepers and erode the medium's openness to innovation.

- Congress should examine and strengthen existing communications privacy laws to cover new services, technologies and business models with consistent rules. ECPA was passed more than 20 years ago, long before there was a World Wide Web and the Internet became integrated into Americans' daily lives. The application of the law to common online activities including Web search remains unclear and the legal protections it provides for the enormous amounts of personal data stored online are far too low.

Conclusion

CDT would like to thank the Subcommittee again for holding this important and forward-looking hearing. We believe that Congress has a critical role to play in ensuring that privacy is protected as deep packet inspection and other new technologies contribute to an increasingly complex online environment. CDT looks forward to working with the Subcommittee as it pursues these issues further.



FOR MORE INFORMATION

Please contact: Leslie Harris, (202) 637-9800, leslie@cdt.org

Mr. BOUCHER. Thank you very much, Ms. Harris.
Mr. McSlarrow.

STATEMENT OF KYLE McSLARROW

Mr. McSLARROW. Mr. Chairman, Mr. Stearns, distinguished members of the subcommittee, thank you for giving me an opportunity to testify today.

I think the starting place for the cable industry is to recognize that Congress passed probably what was at that time the first broad based opt-in statute, a very forward-leaning, pro-consumer, privacy protection regime that we have lived under for over 25 years for cable services. And today with digital voice services, we now live under the similar privacy protections offered under Section 222 of The Communications Act. And during that time I think our track record has been excellent both in terms of safeguarding consumer privacy and abiding by rules that I think people have discovered prove that good privacy protection in also good business so we believe that.

As I think everybody has acknowledged, the question on the table isn't so much what people are doing today. It is about the emerging models and emerging ideas in creativity and what they mean for privacy, and we think it is completely appropriate to examine all of that.

In the short time I have available, I do want to take a deeper dive into deep packet inspection because I think it is actually emblematic of this entire conversation. It is true that today, at least for my members, none of the cable ISPs are actually using any of this information for behavioral targeting purposes. But obviously, there are many industries including ours who are interested in trying to figure out a way to provide more relevant and useful advertising for the consumer. It is likely to support the entire Internet ecosystem. It is likely to spur more growth in creative ideas and content and services, but we recognize that it has to be done in a way that is respectful of the consumer's privacy.

Deep packet inspection is actually not something that is new. One of the frustrations I think we have is that people act like something just happened yesterday, something new and different and scary. Deep packet inspection or packet inspection generally is something the operators, all providers have used or tools like that for many years and for very good reasons. I think the test is consumer expectations and I think broadly speaking, when a consumer sits down at a computer it is always on if they are a broadband customer. They go anywhere they want. They access any application they want. No one stops them. It all works. The speeds are doubling. The price per megabyte is dropping. Deployment is continuing but on the other side of that computer, there is a war going on. You have got network operators who are fighting malware and viruses and spam. You have got botnet armies and things that I don't even know about that are taking place in a very complicated regime. The consumer doesn't know anything about that. They don't want to know anything about that. They don't necessarily need to know how you are dealing with it. They just want you to deal with it and we do.

Now, I think reading everybody's testimony, I think everybody concedes that the use of deep packet inspection has today beneficent and pro-consumer purposes so I am not going to dwell on that. But I will say there it is hard to do analogies because probably no one in this room or very few are really technical experts here. But I do think we have to be very careful. We require some precision here when we are talking about deep packet inspection.

I have heard and I think Leslie just said as an example, this is like the post office opening up your letter, going beyond looking at the address and looking at the contents of the letter. And I myself am guilty sometimes of just saying a packet of information on the Internet has a header and a payload. But the truth is if you are looking at the layers of a packet, each layer has a header and payload. Each, you know, one layer, layer four is going to be something, you know, that has source and destination for IP addresses, all the way down to layer seven where you could have a web browser, URL address, source and destination. And when you hear envelope and content you think there is just one step before you get to the content but the truth is, it is really more like envelopes within envelopes, each one of which has addresses and at some point you do have content.

So far as I can tell, I haven't done my own due diligence, the only time we are actually scanning and what I mean by scan, I mean a machine doing something in a billionth of a second, content is what we are trying to deter spam. All of the other activities related to deep packet inspections so far as I am aware, are looking at headers. That is the addresses that most people say they are actually OK with.

So my point here is just a caution. Any technology can be used for good purposes and for bad. We recognize that no one would want us looking at the communications in an e-mail. We don't particularly want to do that. In fact, the only tracking I actually want to do is to track down the engineer who actually came up with the term deep packet inspection and shoot him.

Last point and I realize I am rowing against the tide here and you do have my commitment, Mr. Chairman, that as you consider legislation to work constructively with you but I do want to make a final plea to consider allowing self-regulation to work and I would really say it for two reasons. Number one, this entire arena is moving so fast. There are new models being created. I know that is what gives rise to the concerns but I also think it is a caution. It is very hard to freeze one point in time with what is actually a fairly immature marketplace when you think about it how young the Internet system is and how young really the broadband market is. And I think we should allow industry and all stake-holders to try to work together using the oversight of this committee and the bully pulpit, force us to come up with self-regulatory principles that respect consumers' privacies knowing that at least in my industry's case, we have a backstop of legislation that gives a lot of the rules of the road. And the second is to recognize that behavioral advertising can potentially be the most pro-consumer thing we do to enrich the Internet to allow new services that haven't even been created yet to survive and thrive by making it easy for those services'

new web applications to monetize their services without having to go out and get the capital necessary to launch a new service.

Thank you, Mr. Chairman.

[The prepared statement of Mr. McSlarrow follows:]

**TESTIMONY OF KYLE McSLARROW
PRESIDENT AND CEO
NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION**

on

Communications Networks and Consumer Privacy: Recent Developments

before the

**Committee on Energy and Commerce
Subcommittee on Communications, Technology and the Internet**

**UNITED STATES HOUSE OF REPRESENTATIVES
WASHINGTON, D.C.**

April 23, 2009

TESTIMONY OF KYLE MCSLARROW**PRESIDENT & CEO, NATIONAL CABLE & TELECOMMUNICATIONS
ASSOCIATION**

Good morning, Chairman Boucher, Ranking Member Stearns, and Members of the Subcommittee. My name is Kyle McSlarrow and I am the President and Chief Executive Officer of the National Cable & Telecommunications Association. Thank you for inviting me today to testify on "Communications Networks and Consumer Privacy: Recent Developments."

NCTA represents cable operators serving more than 90 percent of the nation's cable television households and more than 200 cable program networks. The cable industry is the nation's largest provider of residential high-speed Internet service, having invested more than \$145 billion since 1996 to build two-way, interactive networks with fiber optic technology. Cable companies also provide state-of-the-art digital telephone service to more than 15 million American consumers. Cable operators are committed to delivering an open and satisfying Internet experience to their customers, and the dramatic growth in cable broadband subscribers is evidence of their success in doing so.

Our industry views the protection of our customers' privacy as a fundamental part of our relationship with our customers and central to the success of our businesses. We operate in a highly competitive marketplace, and our ability to succeed depends on winning and retaining the trust of those customers. And as new business models and new network technologies are developed, we will ensure that they are deployed in a manner that respects our customers' privacy.

Cable subscriber privacy is already enshrined in the Communications Act, in a comprehensive consumer protection framework that has been in effect for almost 25 years. This law –

- requires cable operators to provide annual written notice to consumers of the nature of personally identifiable information (“PII”) collected, including clearly and conspicuously describing how it is used, disclosed to others, and maintained;
- prohibits cable operators from collecting PII without prior customer consent, except as necessary to render service and detect service theft, and from disclosing PII without prior customer consent, except as necessary to render services or conduct other legitimate business activities related to rendering service;
- provides detailed requirements governing how subscriber records may be disclosed pursuant to court order;
- requires that subscribers be given access, at reasonable times and convenient locations, to all PII that is collected and maintained, and a reasonable opportunity to correct any errors in PII; and
- requires cable operators to take “such actions as are necessary” to prevent unauthorized access to PII, including destroying it if it is no longer necessary for the purposes for which it was collected and there are no pending court orders or requests for access to such information.

In addition, cable providers of digital voice service comply with the privacy protections of section 222 of the Communications Act regarding customer proprietary network information (“CPNI”).

We welcome the focus of this hearing; nearly all modern technologies – without which broadband networks could not function effectively and efficiently – have a variety of features and attributes that could implicate privacy concerns if misused. We believe the right question is what principles appropriately protect reasonable expectations of consumer privacy in a very complex online environment with many different actors. While it is certainly reasonable to examine how technologies are used, we would respectfully suggest that focusing exclusively on one particular technology – and how it *might* be misused – risks obscuring an informed and reasonable discussion of online

privacy when there are unlimited numbers of technologies and situations that could be hypothesized. What matters are the purposes for which we use those technologies and the principles by which we protect our customers' privacy. We look forward to engaging in that discussion with you.

Behavioral Advertising and Subscriber Privacy

Behavioral advertising has many advantages for consumers. Instead of a barrage of irrelevant ads, subscribers can receive information about services and offerings tailored to reflect their interests. Moreover, advertising remains a critical way to fund content and services online, often for free. Thus, advertising that is more relevant for the consumer is likely to be of more practical value to the consumer and essential to ensure the continued explosion of new content and services.

Currently, none of our cable Internet Service Providers ("ISPs") engages in behavioral advertising – that is, they do not use network-based technologies to collect behavioral data for the purpose of delivering targeted ads. But we believe that achieving and sustaining subscribers' trust requires adherence to a privacy framework that addresses four principles: first, giving customers *control*; second, providing *transparency* and *notice*; third, *safeguarding personal information*; and fourth, providing customers with *value*. And, because of the complexities involved and because the Internet is evolving so quickly, we think it is important for all industry stakeholders to work cooperatively to establish self-regulatory principles. The Federal Trade Commission's recent staff report provides a useful guide to these discussions. We look

forward to working with this Subcommittee, the FTC, and other interested policymakers and stakeholders in developing this framework.

Let me add a word here about “Canoe Ventures.” Canoe Ventures was founded last year by six of the nation’s leading cable operators to develop a national platform for delivering more relevant video advertising to cable television subscribers. These efforts are in the earliest stages, with two services slated for rollout later this year – one that does not involve the collection of any personal information through set-top boxes or otherwise, and one in which the subscriber would specifically and affirmatively consent to receiving additional information about a product or service. When and if Canoe Ventures seeks to use set-top box data to deliver behavioral ads, cable operators will do so in compliance with the privacy requirements applicable to them.

Deep Packet Inspection

As I said at the outset, what matters are the principles that should apply, not the technologies or tools that may be available today or invented tomorrow. Any technology can be used for either benign or nefarious purposes. However, given the concerns raised about deep packet inspection (“DPI”) by some of the other witnesses, I thought it would be useful to explain how cable operators actually use this technology.

Packet inspection serves a number of pro-consumer purposes. First, it can be used to detect and prevent spam and malware, and protect subscribers against invasions of their home computers. It can identify packets that contain viruses or worms that will trigger denial of service attacks; and it can proactively prevent so-called Trojan horse

infections from opening a user's PC to hackers and surreptitiously transmitting identity information to the sender of the virus.

Packet inspection can also be used to help prevent phishing attacks from malicious emails that promote fake bank sites and other sites. And it can be used to prevent hackers from using infected customers' PCs as "proxies," a technique used by criminals, in which user PCs are taken over and used as jumping-off points to access the Internet, while the traffic appears to be generated by the subscriber's PC. As a result, the technology can be used in spam filters and firewalls.

Second, packet inspection can be used for network diagnostics and capacity planning. Cable operators cannot plan for network growth without understanding how Internet traffic is growing and the uses to which it is put. By using this technology to analyze the aggregate growth and usage changes in network traffic patterns over time, cable operators can anticipate the needs of their subscribers and appropriately plan for network growth.

Third, packet inspection can help network operators accurately respond to formal requests from law enforcement agencies for the interception of communications for law enforcement purposes. When law enforcement agencies identify traffic of concern, this technology allows network operators to comply with their legal obligations to flag that traffic.

Finally, the Internet is not static. Different opportunities and challenges will emerge and this technology may prove useful in providing consumers more choice and control in ways that are difficult to predict today. For instance, as streaming video

capabilities increase, this technology could be a means of supporting more advanced parental controls.

Let me stress again that this technology – like any technology we deploy – is being deployed in a manner that respects our customers' privacy. We believe that protection of subscriber privacy is the most useful focus for the policy debate.

Conclusion

NCTA believes that a dialogue addressing online privacy issues is healthy and a necessary component of the ongoing evolution of broadband and online services. But we respectfully suggest these discussions not be focused on one particular technology; rather, the focus should be on principles that both ensure a vibrant Internet that supports current and emerging content and services and also protect consumers' privacy.

NCTA and its members remain committed to working cooperatively and constructively with members of this Subcommittee and other stakeholders to address these issues. Thank you again for the opportunity to appear today.

Mr. BOUCHER. Thank you, Mr. McSillarow.
Mr. Rotenberg.

STATEMENT OF MARC ROTENBERG

Mr. ROTENBERG. Thank you, Mr. Chairman and members of the committee. I appreciate the opportunity to be here today.

EPIC has a broad interest in matters of consumer privacy and network security. We have worked on technical issues at ICANN and IETF on the evolving standards for Internet security. We have been at the FCC on rule-making for consumer privacy and we have even defended the commission's authority to enforce consumer protections on the network. So we have a broad understanding I think of the issues and the opportunities to safeguard consumers in this emerging online environment and I agree very strongly with the members of the committee who say that this is a vital issue for consumers today. According to the Federal Trade Commission, identity theft is the number one concern of American consumers. We have serious problems also with security breaches and so the need to find a policy here that makes it possible to take advantage of new technology to grow new business opportunities and at the same time to safeguard consumers is absolutely critical.

Now, let me say a few words about the DPI issue and I should add I have also been teaching privacy law for many years over at Georgetown. One of the things that has occurred to me is that many of these issues that may seem new today, in fact have been with us for a very long time. So I want to say a few words now about The Communications Act of 1934. The Communications Act of 1934 set out the first regulatory framework for communication service providers in the United States and it tried to answer a simple question, in part. Under what circumstances should communication service providers get content to the information that they are conveying on behalf of their customers. And the answer, generally speaking, was to ensure the provision of the service to make sure that it worked and to protect security and to comply with a legal requirement provided by the government such as a warrant. And there really were no other exceptions which is to say you could listen in on the telephone to make sure your line was working, and you could deal with load leveling issues, and you could enforce a wiretap if you were told to do so but you weren't supposed to access the communications traffic for your own commercial benefit.

And I think that commonsense understanding of the obligations of communication service providers answers most of the questions that have been asked about deep packet inspection today. I do not think that companies that are in the business of providing network services to customers should get access to the content of the communications for a commercial benefit. There may be other good reasons, spam, viruses, legal obligations which I think we would all accept are appropriate exceptions but broadly speaking I don't think there should be access.

Now, here is where it gets interesting. The companies that have come along in the last couple of years such as NebuAd and Phorm have said we have a way to get access to the traffic that doesn't require us to know who the individual users are. We are going to do this type of targeting without collecting personally identifiable

information which from a privacy perspective is actually very attractive because our big concern, of course, is that if companies know who these users are they build very detailed profiles and people just won't know how much information about them is being collected. And so NebuAd and Phorm, both companies that have been highly criticized for their technique are at the same time developing some of the most innovative methods for advertising because they are genuinely concerned about privacy.

Now, this actually creates for you a very interesting dilemma. I don't think it solves the intercept problem because the truth is they are still going to the network without affirmative consent and they are still getting access and I think they are still violating The Wiretap Act as many of the members of this committee concluded last year and as European Commission Vivian Redding said early this month when she brought an action against the Government of Great Britain for allowing the service to go forward. So the intercept problem is still there but the question is let us say people agreed. Let us say people said well if you can do this advertising well and you are not profiling me maybe I am OK with that and I think you still have a policy challenge. I think you have to ensure that these new services really do protect the anonymity of the users, really ensure that it doesn't become possible later to figure out who these folks are or don't simply decide to change the business model.

Now, why should you be concerned about that and why do you ultimately need to legislate because that is actually what happened 10 years ago with online advertising. When a company called DoubleClick said we can make anonymous advertising work on the Internet, many of us supported that. Many companies partnered with DoubleClick and then DoubleClick said well now that we got all of these people in our advertising base, maybe we should start identifying them. And that actually began the first wave of hearings on the issue of Internet privacy when people were being targeted because of who they were without adequate privacy protection. And I think that will be a critical question in this specific context for this committee to address.

Mr. Chairman, if I would make one final point and I very much appreciate the fact that you have held this hearing and plan to hold another hearing, I do think from the user perspective we can't limit the discussion to concerns about DPI. There are a lot of other activities that implicate online privacy, web-based e-mail for example. I mean I am surprised that companies are able to get access to the content of e-mail and provide advertising on that basis. From the user's perspective that is the functional equivalent of the carrier getting access to the message and providing some, you know, commercial benefit. It is a difficult question that hasn't been addressed yet but I hope the committee will get to that one, as well.

Thank you very much.

[The prepared statement of Mr. Rotenberg follows:]



ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Marc Rotenberg
Executive Director, EPIC
Adjunct Professor, Georgetown University Law Center

"Communications Networks and Consumer Privacy:
Recent Developments"

Marc Rotenberg,
EPIC Executive Director

Before the

House Committee and Energy and Commerce
Subcommittee on Communications,
Technology and the Internet

April 24, 2009
2322 Rayburn House Office Building
Washington, DC

Mr. Chairman and Members of the Committee, thank you for the opportunity to testify today on "Communications Networks and Consumer Privacy: Recent Developments." My name is Marc Rotenberg and I am the Executive Director of the Electronic Privacy Information Center (EPIC) and Adjunct Professor at Georgetown University Law Center where I teach Information Privacy Law.

EPIC is a non-partisan research organization, focused on emerging privacy and civil liberties issues. We have a particular interest in communications networks and consumer privacy. EPIC began with a national campaign -- the first online petition -- to protect the freedom to use encryption, a critical technique for network privacy and security. For the past 15 years, EPIC has pursued many of the critical network privacy issues on behalf of Internet users. We have participated in the work of the ICANN on such technical standards as WHOIS¹ and DNSSEC,² and the original IETF review of the RFC for cookie management.³

We also support the authority of the FCC to establish enforceable safeguards for consumers. Over the past decade, EPIC has pursued several complaints at the FCC to promote consumer privacy, to improve security, and to reduce the risk that surveillance standards will jeopardize network integrity.⁴ And EPIC has filed amicus briefs in the courts on many occasions both to safeguard communications privacy and to protect the rulemaking authority of the FCC.⁵ On this last point, I am pleased

¹ EPIC, WHOIS, <http://epic.org/privacy/whois/> (last visited Apr. 22, 2009).

² EPIC, DNSSEC, <http://epic.org/privacy/dnssec/> (last visited Apr. 22, 2009).

³ EPIC, Net Users Urge Standards Group to Protect Privacy, Apr. 7, 1997, *available at* http://epic.org/privacy/internet/cookies/ietf_letter.html.

⁴ *See, e.g.* EPIC, NCTA v. FCC: Concerning Privacy of Customer Proprietary Network Information (CPNI), <http://epic.org/privacy/nctafcc/>; EPIC, Comments of the Electronic Privacy Information Center in the Matter of ACA International Petition for Expedited Clarification, FCC Docket No. 02-278, May 11, 2006, *available at* http://epic.org/privacy/telemarketing/fcc_aca_05-11-06.html.

⁵ *See, e.g.* Brief of the Electronic Privacy Information Center, *U.S. West v. Federal Communications Commission*, 182 F.3d 1224 (10th Cir. 1999) (FCC opt-in privacy rule), *available at* http://epic.org/privacy/litigation/uswest/amicus_brief_SRPR.html; Supplemental Brief, *U.S. v. Councilman*, 418 F.3d 67 (1st Cir. 2005) (No. 03-1383) ("intercept" of stored communications), *available at* http://epic.org/privacy/councilman/kerr_amicus.pdf. *See also*, EPIC, "US West v. FCC -- The Privacy of Telephone Records," <http://epic.org/privacy/litigation/uswest/> (last visited Apr. 22, 2009), EPIC,

to report that the D.C. Circuit Court of Appeals recently upheld an opt-in privacy standard to a challenge brought by the cable companies to an agency rule that we helped develop to safeguard consumers against data brokers.⁶ EPIC filed an amicus in support of the FCC in that case.⁷

Online Advertising

Today I will focus my remarks on growing concerns about consumer privacy and network advertising. I should say at the outset that we do not object to online advertising. We recognize that advertising plays a critical role in enabling the provision of services and information on the Internet. It supports the sites maintained by bloggers and helps enable the free flow of information. Advertising helped launch and maintain the Internet economy.

At the same time, we believe it is becoming clear that that unregulated collection of consumer data is posing an increasing danger to online privacy and maybe even to the economic model itself. A small number of companies and large advertising networks are obtaining an extraordinarily detailed profile of the interests, activities and personal characteristics of Internet users. Users have little idea how much information is gathered, who has access to it, or how it is used. This last point is critical because in the absence of legal rules, companies that are gathering this data will be free to use it for whatever purpose they wish – the data for a targeted ad today could become a detailed personal profile sold to a prospective employer or a government agency tomorrow.

The harm to consumers is not easy to measure. We know there are serious problems in the United States with identity theft⁸ and security breaches,⁹ but there

"United States v. Councilman," <http://epic.org/privacy/councilman/> (last visited Apr. 22, 2009).

⁶ *National Cable and Telecommunications Association v. Federal Communications Commission*, No. 07-1312, slip op. (D.C. Cir. Feb. 13, 2009).

⁷ Brief for EPIC, Privacy and Consumer Organizations, Technical Experts, and Legal Scholars as Amicus Curiae, *National Cable and Telecommunications Association v. Federal Communications Commission*, 555 F.3d 996 (D.C. Cir. 2009) (No. 07-1312); available at <http://epic.org/privacy/nctafcc/epic-ncta-050608.pdf>.

⁸ Federal Trade Commission, 2006 Identity Theft Survey Report, Nov. 2007, available at <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf> (finding that nearly 4% of surveyed Americans were victimized by identity theft in the previous year, and that the resultant costs topped \$15 billion).

⁹ See, e.g.

In the Matter of The TJX Companies, Inc., FTC Docket No. 072-3055 (FTC 2008)

has not been enough work on the specific link between excessive data gathering and the enormous dangers that consumers face in the networked economy. Still, if the TJX case in Massachusetts provides any indication of the scope of the problem, it is clear that current data collection practices do place consumers at risk.¹⁰ And there is every reason to anticipate that these problems will get worse as long as there is little protection for the data that is gathered.

Significantly also for the economics of the online advertising industry, the profiles that are being developed are increasingly untethered from the editorial content of web sites or the business-customer relations that online consumers have with particular companies. By this I mean that advertisers are learning far more about users than the sites that users actually visit or the businesses they actually interact with. This has profound implications for the future of online advertising and the relationship between users, web publishers, and advertising networks.

For example, Google recently announced that it would move to “Interest-based” advertising, which means that the web-based advertising model will be less dependent on the valuable content of web sites and more dependent simply on what Google know about users.¹¹ Google is not the only company to do this, and they have tried to create some privacy safeguards, though in my opinion they are not very effective. But the larger development is the increasing transfer from a customer-business relationship to the user profile-advertiser model. Apart from the privacy problems with this model, there are likely to be also substantial antitrust concerns

(Complaint), available at <http://www.ftc.gov/os/caselist/0723055/080327complaint.pdf> (data breach involving the improper disclosure of personal information concerning approximately 455,000 consumers, and resulting in tens of millions of dollars in claims for fraudulent credit card charges, as well as the cancellation and reissuance of millions of cards); *In the Matter of Reed Elsevier, Inc. and Seisint, Inc.*, FTC Docket No. 052-3094 (FTC 2008) (Complaint), available at <http://www.ftc.gov/os/caselist/0523094/080327complaint.pdf> (data breach leading to criminals acquisition of sensitive information about at least 316,000 consumers, and subsequent use to activate credit cards, open new accounts, and make fraudulent purchases.).

¹⁰ U.S. Federal Trade Commission, *Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data*, March 27, 2008, available at <http://www.ftc.gov/opa/2008/03/datasec.shtm>.

¹¹ Google, *Making ads more interesting*, Mar. 11, 2009, <http://googleblog.blogspot.com/2009/03/making-ads-more-interesting.html> (last visited Apr. 22, 2009).

Testimony of Marc Rotenberg, EPIC
House Commerce Committee,
Subcommittee on Communications

3

“Communications Networks and
Consumer Privacy:
Recent Developments”

and a real question as to whether this approach will sustain web publishers in the long-term.

EPIC attempted to address these issues in a complaint before the Federal Trade Commission in 2007 regarding the Google-DoubleClick merger.¹² I will not go into that topic this morning other than to say that as the Committee considers the privacy risks that arise from networked-based advertising models, I hope you will consider the full range of threats to consumers and also the long-term structure of this market.

Recent Developments

Last year, Members of this Committee drew attention to a new threat to users when it told an online advertising company, NebuAd, to back off a plan to partner with cable and telephone companies.¹³ NebuAd was proposing to use "deep packet inspection" techniques to both profile users based on their Internet activity and to place targeted advertisements. The technology deployed by NebuAd, third-party tracking cookies, was hardly a new technique, but it was more invasive and it took advantage of the ISP's access to network traffic to develop user profiles.

Representative Markey and Representative Barton played a leading role in the effort to stop Charter, a large national cable company, from adopting the NebuAd targeting model. Eventually, the company backed off the plan. Members rightly charged that intercepting network communications ran afoul of the Wiretap Act.¹⁴

These new threats to online privacy are not limited to the United States. Because of the global nature of the networked economy, policy challenges that are

¹² See EPIC, Privacy? Proposed Google/DoubleClick Deal, <http://epic.org/privacy/ftc/google/> (last visited Apr. 22, 2009).

¹³ Letter from Re. Edward J. Markey and Rep. Joe Barton to Mr. Neil Smit (May 16, 2008) ("We are writing with respect to recent media reports that Charter Communications has announced plans to begin collecting information about websites that subscribers visit and then disclosing such data to a firm called NebuAd.") <http://markey.house.gov/index.php?option=content&task=view&id=3401&Itemid=125>

¹⁴ The Wiretap Act provides for civil liability and criminal penalties against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any ... electronic communication [except pursuant to a statutory exception]." 18 U.S.C. § 2511(1)(a) (2009).

arising in the United States are also faced in many countries around the world. In the United Kingdom, the debate over deep packet inspection continues. A company called Phorm has pursued a business model similar to NebuAd. The UK Information Commissioner's Office, somewhat surprisingly, took the position that Phorm's monitoring of user activity did not violate user privacy as long as users had opted-in. That decision did not sit well with UK users, UK online companies, or the European Commission.

Earlier this month, European Commissioner Viviane Redding began legal proceedings against the UK government for violating EU law by allowing Phorm to go forward with its controversial Internet monitoring plan. Commissioner Redding has alleged violations of both the 1995 EU Directive concerning data protection¹⁵ as well as the 2002 EU Directive concerning electronic communication.¹⁶ If the Commission is successful in this challenge, which appears likely, the UK government will be required to change its privacy law so as to ensure that Phorm, and other companies engaged in similar practices, cannot continue to monitor the private activities of Internet users in the UK. In a statement, Commissioner Redding said, "Technologies like Internet behavioral advertising can be useful for businesses and consumers but they must be used in a way that complies with EU rules. These rules are there to protect the privacy of citizens and must be rigorously enforced by all member states."

Several UK firms, including Wikipedia and Amazon, have also announced that they do not want to be included in the Phorm advertising service.¹⁷ While it is good to see these organizations take steps to protect privacy, the opt-out scheme currently in place in the UK is unworkable and will leave users without a clear indication of whether their network traffic is being monitored. That is the reason that a clear legal prohibition must be maintained.

¹⁵ European Commission, "Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data," available at http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Directive&an_doc=1995&nu_doc=46.

¹⁶ European Commission, "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector," available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML>.

¹⁷ Wikimedia Technical Blog, "Wikimedia Foundation opting out of Phorm," (Apr. 16 2009), <http://techblog.wikimedia.org/2009/04/wikimedia-opting-out-of-phorm/> (last visited Apr. 22, 2009); BBC, "Amazon blocks Phorm adverts scan," (Apr. 15, 2009), <http://news.bbc.co.uk/2/hi/technology/7999635.stm>.

Policy Analysis

Companies such as NebuAd and Phorm claim that their techniques protect privacy because they do not necessarily require the collection of personally identifiable information, a traditional trigger for the application of a privacy law. But this observation is not correct with respect to the privacy safeguards required for communication service providers. In the communications context, service providers and their businesses partners also have an obligation not to intercept the content of a communication except for the purpose of providing the service, to comply with a court order or other similar legal obligation.¹⁸

It is possible that the techniques being developed by these firms may help in some ways to safeguard privacy if they are robust, scalable and shown to provably prevent the identification of Internet users. But the essential problem is that they simply do not have the right to access communications traffic for this purpose. Also, I would not recommend that you alter current law or enable consent schemes to make this permissible.

First, companies have not demonstrated the viability of the non-PII model. It is simply too easy to reconstruct actual identity from network traffic. While we remain hopeful that advertising models based on non-personally identifiable information can be made, there are still too many instances where companies, particularly where there is no regulation, fail to fulfill their responsibilities.

Second, even if these privacy techniques are shown to be reliable, it will still be necessary to enact legislation to place the burden on the advertising company to prevent the reconstruction of user identity. Without this statutory obligation, there would be no practical consequence if a company inadvertently disclosed personal information or simply changed its business model to true user-based profiling. In fact, this is exactly what happened in the early days of online advertising when the company Doubleclick moved from an anonymous advertising model that was widely supported to a true user-based targeting scheme.

Third, the long-term consequences of encouraging network-based advertising will likely degrade network security and privacy. For example, it may become more difficult to adopt good network security standards, such as IPsec (Internet Protocol security),¹⁹ if ISPs have a vested interest in access to their

¹⁸ See 18 U.S.C. § 2511(1)(a) (2009); 18 U.S.C. § 2511(1)(c)-(d) (2009); 18 U.S.C. § 2511(3)(a) (2009).

¹⁹ Wikipedia, IPsec, <http://en.wikipedia.org/wiki/IPsec> (last visited Apr. 22, 2009) (describing IPsec as "a suite of protocols for securing Internet Protocol (IP)

customers' network traffic for commercial benefit. Sealing the envelope will make it more difficult to inspect its contents.

There are technical measures that may allow some users to avoid the risks of deep packet inspection. For example, a Secure VPN uses cryptographic tunneling protocols to enable private communications over unsecure networks. There are both proprietary and open standards for Secure VPN. Significantly, the long-delayed Internet Protocol standard IPv6 would include IPsec as a standard.

Congress needs to keep a long-term view of the growth of the Internet. If the claims of Internet advertisers that they must have the unrestricted ability to monetize user traffic goes unchallenged, users will face new privacy risks, web publishers will find that their content is less valuable, and the technical standards that are necessary for the integrity of the Internet will be further delayed. Once down this road, it will be difficult to turn back.

Conclusion

From the user perspective, the threats to privacy online are increasing. Unregulated data collection continues. Privacy policies are opaque and ineffective. Users are unable to exercise any meaningful control over the personal information that is obtained by firms when they visit sites, purchase online, or participate in the rapidly growing world of social networking.

Some have simply given up and said that reduced privacy is the cost of new technology. But even that approach may not work. The Federal Trade Commission reports that identity theft and the related problem of security breaches continue to grow. To give up a privacy protection would allow identity theft and security breaches to escalate even further.

The Committee's oversight on the Deep Packet Inspection matter is commendable, but more needs to be done. There should be greater oversight of practices in the online advertising industry and a greater willingness to distinguish between sensible business practices and those that should not be permitted. Regarding many of these new challenges, I recommend in particular the work of the Center for Digital Democracy. Mr. Jeff Chester has brought attention to fundamental

communications by authenticating and encrypting each IP packet of a data stream. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.")

Testimony of Marc Rotenberg, EPIC
House Commerce Committee,
Subcommittee on Communications

7

"Communications Networks and
Consumer Privacy:
Recent Developments"

changes in online advertising that are generally not well understood by the American public and that pose a real threat to the open evolution of the Internet

We also look forward to the development of the FCC's National Broadband Plan. The Commission and the Acting Chair have identified privacy as a top concern in the development of this important initiative. We agree and believe that consumers across the country want the assurance that when they use new technology their personal information will be protected and they will not be profiled and tracked by secretive companies, hiding in the shadows of the Internet.

Thank you again for the opportunity to appear before the Committee today. I will be pleased to answer your question.

ADDITIONAL REFERENCES

EPIC, "NCTA v. FCC: Concerning Privacy of Customer Proprietary Network Information (CPNI))" ("Federal Appeals Court Upholds Opt-In Privacy Rule for Telephone Services." Feb. 13, 2009)
<http://epic.org/privacy/nctafcc/>

EPIC, "Deep Packet Inspection and Privacy"
<http://epic.org/privacy/dpi/>

EPIC, "FCC Approval of FBI Wiretap Standards Threaten Communications Privacy," (Aug. 27, 1999)
http://www.epic.org/privacy/wiretap/calea/comments_12_98.html

EPIC Letter to FCC Chairman Martin, May 17, 2006 ("If telecommunication carriers disclosed customer information to the NSA in the manner described in press reports, then violations of section 222 of the Communications Act have occurred.")
<http://www.epic.org/privacy/wiretap/epic-fcc-nsa.pdf>

FCC, Report and Order and Further Notice of Proposed Rulemaking, Adopted: March 13, 2007 - Released April 2, 2007: "Our Order is directly responsive to the actions of data brokers, or pretexters, to obtain unauthorized access to CPNI. As the Electronic Privacy Information Center (EPIC) pointed out in its petition that led to this rulemaking proceeding, numerous websites advertise the sale of personal telephone records for a price. These data brokers have been able to obtain private and personal information, including what calls were made to and/or from a particular telephone number and the duration of such calls. In many cases, the data brokers claim to be able to provide this information within fairly quick time frames, ranging from a few hours to a few days. The additional privacy safeguards we adopt today will sharply limit pretexters' ability to obtain unauthorized access to this type of personal customer information from carriers we regulate. We also adopt a Further Notice of Proposed Rulemaking seeking comment on what steps the Commission should take, if any, to secure further the privacy of customer information."
http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.doc

Mr. BOUCHER. Thank you, Mr. Rotenberg.
Ms. Attwood.

STATEMENT OF DOROTHY ATTWOOD

Ms. ATTWOOD. Thank you, Chairman Boucher and Ranking Member Stearns for providing AT&T the opportunity to discuss consumer privacy in the online world.

As the leading communications company in America, AT&T has a profound interest as a major advertiser, as a Web site publisher, as an Internet service provider and as a provider of communications generally, in seeing the Internet grow through an advertising-supported model. After all, online advertising fuels investment and innovation across a wide range of Internet activities and next generation forums of online advertising could prove quite valuable to consumers and could dramatically improve their online experiences.

At the same time, we balance our interest in the evolution of online advertising with the unique investment we have in concentration on our customer relationships. These relationships are our most treasured asset and we are doggedly focused on enhancing them and ensuring that our customer expectations are met. For this reason, AT&T has articulated and publicly supports a pro-consumer framework that both promotes the privacy interests of our customers as well as fostering advancements that lead to more useful and relevant online advertising. We have endorsed the simple principle that we need to engage consumers and offer them transparency and control over their Internet experience.

The new forms of online advertising that is the subject of today's hearing which we generally refer to as behavioral advertising, can take many forms. They can in theory involve the use by an ISP of technologies such as deep packet inspection to capture and analyze a user's Internet browsing activities and experience across unrelated Web sites. They also involve search engines and advertising networks implementing evermore sophisticated technologies to track consumer web surfing and search activity over time, to develop profiles of consumer activity and combine data from offline and online sources. They are not inherently problematic but pitfalls can arise because behavioral advertising in its current forms is largely invisible to customers.

We have actually conducted focus groups and we have asked our customers their views on behavioral advertising and the results have been illuminating. Customers clearly appear to understand and willingly accept that information will be collected in commercial relationships and will be used to offer goods and services that are of value to them. But these same consumers do not well understand and fully embrace the concept that their online activity associated across unrelated Web sites or their overall web browsing activity can be and is used today to create detailed profiles of them. They can see the benefits of more targeted and relevant advertising but they want control over their personal information and they want that control to be individualized.

These new online advertising paradigms must therefore be designed to account for a new set of still evolving customer expectations about how personal information will be used and how per-

sonal privacy will be safeguarded. As an industry then, we must deploy next generation advertising techniques in tandem with next generation privacy innovations and any solution must be achieved by all elements of the Internet ecosystem.

For its part, AT&T is listening to its customers and we are confronting the opportunities and challenges presented by behavioral advertising by not thoughtlessly lurching into this realm. We will initiate such a program only after testing and validating the various technologies and only after establishing clear and consistent methods and procedures to engage customers, to ensure the protection of and ultimately their control over their information. If AT&T deploys these technologies and processes, we will do it the right way. So indeed, AT&T has already adopted flexible privacy principles that will guide any effort to engage in behavioral advertising, the pillars of which are transparency, customer control, privacy protection and customer value. These principles can be the foundation of an ethic of consumer engagement for all players in the online behavioral advertising sphere and it both ensures that customers have ultimate control over the use of their personal information and guards against privacy abuse.

I want to thank you very much and look forward to your questions.

[The prepared statement of Ms. Attwood follows:]

**STATEMENT OF DOROTHY ATTWOOD
SENIOR VICE PRESIDENT, PUBLIC POLICY & CHIEF PRIVACY OFFICER
AT&T INC.**

BEFORE:

**SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY & THE INTERNET
COMMITTEE ON ENERGY & COMMERCE
UNITED STATES HOUSE OF REPRESENTATIVES**

HEARING ON COMMUNICATIONS NETWORKS AND CONSUMER PRIVACY

April 23, 2009

Thank you, Chairman Boucher and Ranking Member Stearns, for providing AT&T Inc. the opportunity to discuss consumer privacy in the online world. As you know, next-generation forms of targeted online advertising – commonly referred to as “behavioral advertising” – raise important privacy issues that are worthy of thoughtful consideration by policymakers and dictate a cautious, consumer-focused approach by industry.

To be sure, your further inquiry into these matters is warranted. The interactive advertising industry continues to grow and experiment with new business models, and new ways of addressing privacy concerns. The attention of Congress, as well as the FTC, to these matters has gone far to encourage industry innovation and robust self-regulation. Your continued engagement in and growing understanding of this topic should, therefore, spur refinement of the technologies, policies and practices that online advertisers adopt.

Today’s hearing is also quite timely. While the companies represented here today generally are not engaged in behavioral advertising, the companies that are not present – most notably search engines and online advertising networks – have moved well past experimentation and have deployed sophisticated methods of tracking, targeting and delivering advertising to online consumers. Thus, we respectfully encourage the committee to focus similar attention on

the actors in the online ecosystem that are today actually engaged in behavioral and other forms of next-generation online advertising. Otherwise, your understanding of these new modes of advertising, their impact on consumers, and the best practices that can and should be utilized to ensure personal privacy, will be incomplete.

The Challenge Posed by Behavioral Advertising

Given AT&T's multi-faceted position as a major advertiser, a website publisher, an Internet service provider ("ISP"), and the leading communications company in America, we have a profound interest in seeing the Internet grow through an advertising-supported model. For this reason, AT&T has articulated and publicly supports a pro-consumer framework that promotes the privacy interests of our customers and fosters the advancements that lead to more *useful and relevant* advertising. We have endorsed the simple principle that we need to engage consumers and offer them transparency and control over their Internet experiences. Next-generation forms of online advertising could prove quite valuable to consumers and could dramatically improve their online experiences. After all, online advertising fuels investment and innovation across a wide range of Internet activities, and provides the revenue that enables consumers to enjoy many free and discounted services and a rich diversity of content and information. Our joint goal should, therefore, be to improve the Internet experience for consumers while also increasing the capabilities of and the consumer value created by the online advertising industry.

Behavioral advertising can take many forms. It can, in theory, involve the use by an ISP of technologies to capture and analyze a user's Internet browsing activities and experience across unrelated websites. Various interactive advertising technologies also allow search engines and advertising networks to implement ever more sophisticated business models to track consumer web surfing and search activity over time, develop profiles of consumer activity, and combine

data from offline and online sources. These techniques include, by way of example, an ad network “dropping” third-party tracking “cookies” on a consumer’s computer to capture consumer visits to any one of thousands of unrelated websites; embedding software on PCs; or automatically downloading applications that – unbeknownst to the consumer – log the consumer’s full session of browsing activity.

Yet, the concern here is not necessarily that there will be more or new forms of online advertising. Rather, pitfalls arise because behavioral advertising in its current forms is largely invisible to consumers. Consumers confront an overwhelming amount of online content and advertising without the benefit of a cohesive explanation of the businesses or relationships that underlie that content, the manner in which the consumer’s personal information is collected or used, or the control – or lack thereof – that the consumer has over her personal information in the first place. Against this backdrop, then, customers clearly appear to understand and willingly accept that information will be collected in commercial relationships – both offline and online – and will be used to offer goods and services that are of value to them. But it seems equally clear that these same consumers do not well understand or fully embrace the concept – what we now call “behavioral advertising” or “invisible tracking” – that their online activity associated across unrelated websites, or their overall web-browsing activity, can be and is used to create detailed profiles of them. These new online advertising paradigms must be designed to account for a new set of still evolving consumer expectations and understandings about how personal information will be used and how personal privacy will be safeguarded. As an industry, then, we must deploy next-generation advertising techniques in tandem with next-generation privacy innovations, and any solutions must be achieved by all elements of the Internet ecosystem.

AT&T's Response to the Challenge

The first thing that AT&T is doing to address the challenge of behavioral advertising – its promise and potential pitfalls – is to avoid thoughtlessly lurching into this realm without proper due diligence. We will initiate such a program only after testing and validating the various technologies and only after establishing clear and consistent methods and procedures to engage consumers and ensure the protection of, and ultimate consumer control over, consumer information. To this end, we are working with privacy advocates, consumer privacy coalitions and fellow industry participants in a cooperative, multi-faceted effort to develop a predictable framework in this area. If AT&T deploys these technologies and processes, it will do so the right way.

Indeed, AT&T already has adopted flexible privacy principles that will guide any effort to engage in behavioral advertising. We summarize this consumer-centric framework as follows:

- **Transparency:** Consumers must have full and complete notice of what information will be collected, how it will be used, and how it will be protected.
- **Consumer Control:** Consumers must have easily understood tools that will allow them to exercise meaningful consent, which should be a sacrosanct precondition to tracking online activities to be used for online behavioral advertising. AT&T will not use consumer information for online behavioral advertising without an affirmative, advance action by the consumer that is based on a clear explanation of how the consumer's action will affect the use of her information. This model differs materially from the default-based privacy policies that advertising networks and search engines – which already are engaged in behavioral advertising – currently employ.

- **Privacy protection:** The privacy of consumers and their personal information will be vigorously protected, and we will deploy technology to guard against unauthorized access to personally identifiable information.
- **Consumer Value:** The consumer benefits of a behavioral advertising program include the ability to receive a differentiated, secure Internet experience that provides consumers with customized Internet advertisements that are relevant to their interests. But we think the future is about much more than just customized advertising. Consumers have shown that in a world of almost limitless choices in the content and services available on the Internet, they see great value in being able to customize their unique online experience. That is the ultimate promise of the technological advances that are emerging in the market today.

The pillars of this framework – *transparency, consumer control, privacy protection, and consumer value* – can be the foundation of an ethic of consumer engagement for all players in the online behavioral advertising that both ensures that consumers have ultimate control over the use of their personal information and guards against privacy abuses. We believe these principles offer a rational approach to protecting consumer privacy while allowing the market for Internet advertising and its related products and services to grow.

Regardless of any ultimate policy framework, though, in order for consumers truly to be in control of their information, *all* entities involved in Internet advertising, including ad networks, search engines and ISPs, will need to adhere to a consistent set of principles. A regime that applies only to one set of actors will not protect consumers. In addition, it will arbitrarily favor one business model or technology over another. After all, consumers do not

want information and control with respect to just a subset of potential online advertising or the tracking and targeting that might underlie those ads. Thus, we trust that the committee will evaluate all facets of the online advertising industry and ensure that any privacy protections apply across the industry and across technologies.

###

Mr. BOUCHER. Thank you very much, Ms. Attwood.
Mr. Scott.

STATEMENT OF BEN SCOTT

Mr. SCOTT. Thank you, Chairman Boucher and Ranking Member Stearns and members of the subcommittee.

I am the policy director for Free Press. We are the largest public interest organization in the country that works on media policy issues. I would like to focus my testimony this morning on deep packet inspection or DPI. I have submitted a white paper on the subject for the record which I will try to summarize here.

You have already heard about the uses for DPI for the collection of personal information about Internet users for advertising purposes. I would like to focus on other issues of DPI technology because really any time a network monitors Internet traffic as Mr. Rotenberg pointed out, we have a potential privacy problem. That harm is compounded by DPI tools that violate network neutrality with any competitive practices.

Let me offer a little context. It is 3 years ago we had a robust debate in the Congress over the necessity of net neutrality and privacy rules to protect the consumers, and that debate largely turned on whether or not the harms were hypothetical, and indeed the technology did not exist in 2006 that would have permitted wide-scale violations. Today these technologies do exist. They are deep packet inspection devices and they are now widely deployed. Worse still, from my perspective, an entire industry of manufacturers has emerged that markets DPI explicitly to monitor and control consumer behavior online. All a network operator has to do is flip the switch.

DPI will have a broad impact on the Internet. Without this technology, everything you do online is sent through the network basically anonymously, e-mail, sports scores, family photos. The network doesn't know or care what you are doing. Online anonymity in this sense also has the virtue of nondiscrimination. But with DPI, it is a whole new ballgame. This technology can track every online click. Once a network owner can see what you are doing, they have the power to manipulate your experience. They can sell you ads. They can block content. They can speed things up. They can slow things down. Perhaps there is no better way to describe what DPI can do then to quote directly from the manufacturers' marketing materials. Their selling points are exactly the uses that trouble me most.

Let me offer a few examples. Zeugma Systems describes its technology as a way for network owners to "see, manage and monetize individual flows to individual subscribers." A company called Allot promises that their equipment empowers ISPs "to meter and control individual use of applications and services" including to help network owners "reduce the performance of applications with negative influence on revenues (e.g. competitive VoIP services)." Now, that sounds like blatantly anti-competitive behavior to me. ProCera Networks went so far as to publish a brochure that was titled "If You Can See It, You Can Monetize It." That is chilling stuff and there are more than a dozen of these companies. I could go on and

on. They sell products marketed to help ISPs make more money by spying on consumers and controlling how they use the Internet.

Let me be clear, the technology itself is not necessarily problematic. However, in the past year deep packet inspection has evolved from basically innocuous to potentially insidious. DPI was created as a network security tool but has become a mechanism of precise surveillance and content control. We have already begun to see incidents of bad behavior.

This subcommittee has had hearings on Comcast and NebuAd which both used DPI in secret, questionable ways. Today, Cox Communications is using DPI to speed up some applications and slow down others. These types of practices may have short term traffic management benefits but the tradeoff is the unprecedented step of putting a network owner in control of consumers' online choices. After this first step, it is a slippery slope. We could soon see every major ISP in the country adopt a different traffic control regime. Without oversight, this could vulcanize the Internet so that applications that work on a network in Virginia may not work on a network in Kansas or Florida.

The critical question is how to best protect consumers from these kinds of harms. Let me offer an analogy. Think of DPI technologies as similar to complex financial instruments like, I don't know, credit default swaps. Properly regulated they can be used as a constructive part of our banking system. But without oversight, they can run amuck and severely harm consumers.

What we need are bright line rules of consumer protections. The negative implications for privacy network neutrality are already clear but the new uses of DPI may also reduce incentives for infrastructure investment. Installing DPI offers a tempting alternative to building a robust network. At a fraction of the cost, a DPI can discourage users from high-bandwidth applications or charge higher fees for priority access.

Before these technologies become firmly entrenched, we encourage Congress to open a broad inquiry to determine what is in the best interest of consumers. Once DPI devices are activated across the Internet, it will be very difficult to reverse course.

I thank you for your time and I do look forward to your questions.

[The prepared statement of Mr. Scott follows:]

MASSACHUSETTS
40 main st, suite 301
florence, ma 01062
tel 413.585.1533
fax 413.585.8904

WASHINGTON
501 third street nw, suite 875
washington, dc 20001
tel 202.265.1490
fax 202.265.1489



Testimony of

**Ben Scott
Policy Director
Free Press**

before the

**U.S. House of Representatives
Subcommittee on Communications, Technology, and the Internet of the
Committee on Energy and Commerce**

Regarding

Communications Networks and Consumer Privacy: Recent Developments

April 23, 2009

SUMMARY

On behalf of Free Press, I appreciate the opportunity to testify on the use of Deep Packet Inspection technologies in broadband networks. As a public interest organization, Free Press advocates for policies that will bring maximum benefit to the consumers of Internet access, services, and content. We have long supported policies to bring Americans universal, affordable access to the Internet – as well as policies to maintain its open marketplace for ideas and commerce. We have strong concerns about the growth of Deep Packet Inspection (DPI) technologies and the intentions of carriers that have deployed them. The technology itself is not necessarily problematic. However, when it is used inappropriately, it has the potential to seriously damage the vibrant Internet marketplace for online content and services.

This is a relatively nascent market, but the way new DPI devices are being designed, marketed and utilized raises questions about anticompetitive activity, violations of consumer privacy, and a fundamental distortion of the Internet's open market that consumers have enjoyed for many years. In the last year, we have witnessed a surge in bad behavior by Internet service providers (ISPs) using DPI. They have monitored consumer behavior online to sell advertising based on behavior tracking; they have secretly blocked legal Internet content from consumers' computers; and they have begun to discriminate between different kinds of online content, giving consumers no say in the matter. The grand plans of the DPI manufacturers include using their technology to monitor and monetize every use of the Internet in order to increase short-term profit margins by limiting investment in network facilities and capturing a toll on Internet commerce. Used for these purposes, these invasive technologies threaten innovation, consumer choice, and privacy for every user of the Internet.

Before these technologies are widely deployed and activated, we encourage Congress to open a broad inquiry to determine what is in the best interest of consumers. Once these new devices are in active use across the Internet ecosystem, it will be very difficult to reverse course. We thank the Subcommittee for taking the lead in scrutinizing the risks DPI poses for consumers.

Deep Packet Inspection – From Innocuous to Insidious

Deep Packet Inspection, or DPI, has evolved dramatically in recent years. It was created as a tool to protect network security by detecting and blocking viruses and denial of service attacks. But it has become a mechanism of precise control – a technology capable of examining huge flows of Internet traffic to and from users in real time. The ramifications of this transformation are only now becoming clear. Without using DPI, Internet service providers simply read the top level of routing information on any packet of data passing through the network. This is akin to the US Postal Service reading the address on the outside of envelopes in order to ensure they reach their proper destination. DPI allows for the ISP to open every packet, read its full contents in real time, and treat that packet differently according to what is in it (e.g. adding advertising information, collecting data about users, or blocking the content altogether.) This is as if the post office created a side business by opening every letter, reading its contents before home delivery, and gathering saleable information—all without the knowledge or consent of the sender or recipient.

The deployment of DPI devices capable of reading high volumes of traffic in this way is a relatively recent phenomenon. But the negative implications for consumer privacy and network neutrality are already clear. DPI permits an extraordinary transfer of power from the edges of the network to the

center—allowing the network operator to play the role of all-knowing gatekeeper between consumers and the Internet.

The debate over network neutrality (and its related concerns over consumer privacy), considered hypothetical by many in 2006 when the first draft bills were circulated, is all too real now. In fact, the Federal Communications Commission spent months in 2008 evaluating Comcast's use of DPI to close off a few specific uses of the Internet.¹ This Subcommittee has dealt with abuses of DPI as well. In the summer of 2008, both the House² and the Senate³ held hearings to evaluate Charter Communications' partnership with NebuAd, designed to examine Internet traffic in real time, look at content in the web pages viewed by the consumer, and insert targeted advertising into the data stream. For both Comcast and NebuAd, the anti-consumer behavior was stopped, but the DPI industry marches on, building ever more powerful and more tempting tools.

The Uses and Abuses of DPI

For network operators, the new uses of DPI promise to increase revenue while decreasing infrastructure investment; but, for consumers, DPI promises higher bills, fewer choices, and less privacy on the Internet. The capabilities of these technologies to yield extraordinary short term revenue at the expense of long term consumer welfare are stark and brazenly promoted by DPI manufacturers. A company is unlikely to invest in infrastructure if DPI permits them to earn higher returns at lower cost by charging a premium for users to access high-bandwidth applications or routing their own preferred content along a faster path versus competitors. Beyond that, an ISP can capture an incredibly rich revenue stream of behavioral advertising by gathering data on *everything* a user does online. However, we should not expect to see DPI's first widespread use in a case of aggressive network control and anti-consumer activity. The descent on the slippery slope of DPI technologies will begin with practices that seem plausibly reasonable but set a precedent that undermines consumer choice and consumer privacy.

Consider the example of Cox Communications. Cox is currently engaging in trials of a network management system that uses DPI to classify Internet communications into high and low priority, based on the application the consumer is using.⁴ Cox intends to use this technique to alleviate congestion problems in its network by selectively slowing down some traffic. Even if we assume the best possible motivation for Cox, another company might use the same technology and the same rationale to avoid network infrastructure upgrades by making it harder for consumers to use the Internet's higher bandwidth applications. Cox's use of DPI to change the routing system of Internet

¹ *In re Formal Complaint of Free Press & Public Knowledge Against Comcast Corp. for Secretly Degrading Peer-to-Peer Applications; Broadband Industry Practices; Petition of Free Press et al. for Declaratory Ruling That Degrading an Internet Application Violates the FCC's Internet Policy Statement & Does Not Meet an Exception for "Reasonable Network Management,"* WC Docket No. 07-52, Memorandum Opinion and Order, FCC 08-183 (Aug. 20, 2008) (Comcast Order).

² See, e.g., Grant Gross, *Lawmakers Call on NebuAd to Change Privacy Notification*, PCWORLD (July 17, 2008), at http://www.pcworld.com/businesscenter/article/148555/lawmakers_call_on_nebuad_to_change_privacy_notification.html.

³ See, e.g., Nate Anderson, *NebuAD CEO defends web tracking, tells Congress it's legal*, ARS TECHNICA (July 9, 2008), at <http://arstechnica.com/news.ars/post/20080709-nebuad-ceo-defends-web-tracking-tells-congress-its-legal.html> ("Dorgan noted that neither he nor most consumers 'have the foggiest idea' about what's being tracked, how long it's maintained, and what it's being used for.").

⁴ See generally Cox Communications, *Congestion Management FAQs*, at <http://www.cox.com/policy/congestionmanagement/>.

content sets a critical and troubling precedent – the choice of which applications work best now lies with the network, not the end user. If this brand of consumer traffic manipulation is acceptable, why not one that takes a step further to prioritize content for commercial advantage or to track consumer behavior? In a market where consumer choices for ISPs are slim and switching costs are high, it is easy to see why this kind of control could lead to negative long term consequences for the Internet economy in exchange for short-term gains for the network owner.

The potential uses and abuses of DPI go far beyond the harms of Comcast, NebuAd, and Cox. DPI enables ISPs to monitor and monetize the Internet at the most fine-grained level. The manufacturers of DPI and related equipment describe it best. We need only to look at their sales materials to see exactly what they have in mind. Their clear intent is to aid in anticompetitive activity and violations of consumer privacy.

Andrew Harries, CEO of Zeugma Systems, wants to help ISPs “see, manage and monetize individual flows to individual subscribers.”⁵ Promotional materials from Allot allege the equipment empowers ISPs “to meter and control individual use of applications and services”⁶ – including to help realize the “Service Provider Need[]” to “reduce the performance of applications with negative influence on revenues (e.g. competitive VoIP services).”⁷ ProCera Networks went so far as to publish a brochure with the title “If You Can See It, You Can Monetize It.”⁸ The intent of the DPI industry is clear – help ISPs make more money by spying on consumers, controlling how they use the Internet, and scrapping the Internet’s open platform for a system of tollbooths.

The Implications for Consumers

The ramifications of abuse of DPI for consumers are frightening. DPI reduces consumer privacy; limits innovation; closes off the Internet; and threatens the online market for commerce and speech.

- *Privacy Violations.* Through DPI, Internet service providers possess the capacity to read, log, and analyze every single Internet packet – and advertisers stand ready to pay highly for the information, with greater value and thus larger rewards going for more personalized and more private information.
- *Anti-competitive Activity.* Increasing innovation in high-bandwidth Internet applications such as online video may undermine the business models of other services offered by the ISP—such as cable TV. ISPs could easily use DPI and other methods, such as metering, to limit the growth of online video and other applications. This practice would keep infrastructure investment low and protect parallel, non-Internet revenue streams in cable television and new kinds of subscription services. The policy issues involved in the gradual transition from old media to new media business models will squarely confront DPI technologies.

⁵ Carol Wilson, *TelcoTV: Zeugma, Roku team on enhanced Net video*, TELEPHONY ONLINE (Nov. 13, 2008), available at <http://telephonyonline.com/iptv/news/enhanced-net-video-1113/>.

⁶ Allot Communications, *Subscriber Management Platform*, available at <http://www.ipnetworks-inc.com/pdfs/allot/Allot%20SMP%20Datasheet.pdf>.

⁷ Allot Communications, *Pushing the DPI Envelope* (June 2007), available at <http://www.sysob.com/download/AllotServiceGateway.pdf>.

⁸ ProCera Networks, *If You Can See It, You Can Monetize it*, available at http://www.proceranetworks.com/images/documents/procera_brochure_web_0620.pdf.

- *Closed Markets:* The value of the Internet lies in its openness – the knowledge that any legal content is available, and that any legal application can be used according to well known standards. This freedom encourages Internet users to explore, and Internet developers to create. DPI can turn the Internet into the ultimate walled garden – applications, services, and even content that do not benefit the service provider’s bottom line may risk being blocked or, if not blocked, slowed to let the “preferred” traffic take priority. These are the classic issues of network neutrality – and the technologies with the power to break the open Internet are now openly marketed and widely deployed.
- *Balkanizing the Internet:* DPI technology on an individual network creates substantial harms by itself; different DPI systems in place on many interconnected networks may be even worse, turning the Internet into just a group of different, loosely connected networks. Uncertainty surrounding the behavior of applications or the availability of content generates obstacles and barriers in the online market for commerce and speech. Through the multiplication of network practices using DPI, we could easily witness the balkanization of the Internet – a disaster for developers and consumers of next generation Internet applications.

The Internet as an Infrastructure

The abuses of DPI, along with many other recent non-DPI issues such as the growing popularity of metered billing at rates likely well above marginal cost, are symptoms of a larger policy problem – the failure of network operators to join Congress in treating the Internet itself as an infrastructure. The Internet is not an entertainment product to be commoditized and consumed – it is a vehicle for economic growth and civic participation. The purpose of broadband policy is, first and foremost, to promote the Internet’s generativity, not the profit margins of the ISPs. However, deregulation of broadband services has created an effective duopoly, one that serves its own interests to preserve and grow its market power, leading to anticompetitive practices and DPI-driven, anti-consumer solutions to problems that are better fixed by continued investment in and expansion of the Internet. The question of how DPI technologies are deployed and utilized will be a critical testing ground for whether or not we are serious about creating a 21st century communications infrastructure.

Conclusion

We have already seen substantial consumer harm as a result of the use and abuse of Deep Packet Inspection technology in Internet networks – and, if the DPI industry’s dreams come true, it seems we haven’t seen anything yet. Attempts to increase broadband competition have failed, resulting in a weakly competitive duopoly in which consumers lack the power to effectively resist these developments. Public policy must step in to fill the void. The Internet is the 21st century infrastructure of information economy. We cannot permit its long-term sustainability to be weakened, balkanized, or cashiered in the name of quarterly returns. Instead, we should work with consumers and network owners to find acceptable, beneficial uses of these technologies.

There are many possible avenues to continue exploring these dangers and possible solutions. As the investigation continues down these paths, we urge the Subcommittee to place the interest of the public first and foremost. The Internet as infrastructure must be preserved, to protect it as a source of innovation and social and economic value unlike any other media in human history. We submit

for the record a recent white paper on this subject that offers a more detailed analysis of DPI technologies and the risks they pose for consumers.

We look forward to working with the industry and the Subcommittee to seek constructive solutions to these concerns.

Deep Packet Inspection:

THE END OF
THE INTERNET AS
WE KNOW IT?

M. Chris Riley
and Ben Scott
Free Press
March 2009

freepress 
www.freepress.net

TABLE OF CONTENTS

3	<i>Introduction</i>
4	<i>DPI History: Comcast and NebuAd</i>
4	Comcast and Internet Blocking
5	NebuAd and Internet Monitoring
6	<i>The Present Day: Prioritization on the Internet</i>
6	Cox Communications
6	Queuing Winners and Losers
7	Risks to Innovation and the Internet
9	ZillionTV: The Future of Discrimination?
10	<i>The Future: Monitoring and Monetizing Through DPI</i>
10	Marketing DPI to Internet Service Providers
13	DPI Shortchanges Consumers
15	<i>Endnotes</i>

INTRODUCTION

During the explosive rise of the Internet, one fundamental principle governed: All users and all content were treated alike. The physical network of cables and routers did not know or care about the user or the content. The principle of nondiscrimination, or “Net Neutrality,” allowed users to travel anywhere on the Internet, free from interference. Nondiscrimination, in various forms, has been a foundation of communications law and policy for decades.

In the early days of the Internet, nondiscrimination was easy to uphold because it was not technologically feasible for service providers to inspect messages and evaluate their content in real time. But recently, electronics manufacturers have developed so-called Deep Packet Inspection (DPI) technology capable of tracking Internet communications in real time, monitoring the content, and deciding which messages or applications will get through the fastest.

Here’s how it works: Messages on the Internet are broken down into small units called packets. Each packet contains a header and a data field. The header contains processing information, including the source and destination addresses. The data field contains everything else, including the identity of the source application (such as a Web browser request, a peer-to-peer transfer, or an e-mail), as well as the message itself (part of the contents of a Web page, file or e-mail). Packets are much like letters – the outside of the envelope is like the packet header, and the inside, like the data field, carries the message.

Historically, Internet communications were processed using only information in the header, because only that information is needed to transfer packets from their source to their destination. By contrast, DPI technology opens and reads the data field in real time, allowing network operators to identify and control, at a precise level, everyday uses of the Internet. Operators can tag packets for fast-lane or slow-lane treatment – or block the packets altogether – based on what they contain or which application sent them.

The first DPI devices were used for manual troubleshooting of network problems and to block viruses, worms and Denial of Service attacks. Initially, DPI was not powerful enough to monitor users’ Internet communications in real time. But today, DPI is capable of far more than security – it enables new revenue-generating capabilities through discrimination.

This new use of DPI is changing the game. In fact, improper use of DPI can change the Internet as we know it – turning an open and innovative platform into just another form of pay-for-play media. Although early uses of real-time DPI by ISPs have been geared toward targeted advertising and reducing congestion, manufacturers market the technology for its ability to determine and control every use of a subscriber’s Internet connection. When a network provider chooses to install DPI equipment, that provider knowingly arms itself with the capacity to monitor and monetize the Internet in ways that threaten to destroy Net Neutrality and the essential open nature of the Internet.

DPI HISTORY: COMCAST AND NEBUAD

The principle of nondiscrimination on the Internet has been codified in law in different ways over the past 20 years. In the first years of network technologies, when users connected to the Internet exclusively over telephone lines, the law of nondiscrimination was carried over from telephone regulations. The rules in place at the Federal Communications Commission prohibited “unjust and unreasonable discrimination” in the operation of phone service.¹ Known as “common carriage,” this regime governed network services for decades until the advent of broadband Internet access services led Congress and the FCC down another path.

Under intense pressure from incumbent phone and cable companies, the FCC moved ISPs out from under common carriage regulations, effectively lifting their nondiscrimination obligations.² But the FCC also issued an *Internet Policy Statement*, declaring that it would protect the rights of Internet users to access the content and attach the devices of their choice.³ The decision to swap out regulations for principles was based, in part, on assurances major broadband providers gave to the FCC that they would not discriminate.⁴ But soon after, network operators began to concoct plans to create new revenue streams by speeding up certain content at the expense of other content – in other words, discriminating.⁵ A major legislative debate followed in Congress – with cable and phone companies lining up on one side and public interest groups and Internet innovators on the other – as to whether to reinstate nondiscrimination rules (aka “Net Neutrality”) or to terminate them permanently. The outcome was a deadlock, leaving the *Internet Policy Statement* as the only remaining line of defense for Internet users.

COMCAST AND INTERNET BLOCKING

A series of events in 2007 led to a high-profile case at the FCC testing the strength of the *Internet Policy Statement*. It began when Comcast users started posting complaints on user message boards about the cable operator’s treatment of peer-to-peer traffic. Though no one could identify quite how it was happening, it appeared that Comcast was blocking file transfers between users. Robb Topolski, a network engineer in Portland, Ore., cracked the code with a series of experiments in the fall of 2007. Additional tests were done by Topolski, the Associated Press and the Electronic Frontier Foundation, which collectively determined that Comcast was using DPI technology to identify packets coming from peer-to-peer applications. Comcast was then secretly blocking those packets, while allowing other packets to pass through unimpeded. Comcast’s actions presented a clear case of network discrimination.

In November 2007, Free Press and other public interest organizations filed a petition with the FCC to demand that Comcast’s activities be stopped and ruled unlawful.⁶ After two public hearings, substantial media attention, and overwhelming public opposition to the practice, the FCC ruled against Comcast and ordered a halt to the company’s blocking practices.⁷ The ruling was a major victory for backers of Net Neutrality. However, the FCC’s order fell short of making Net Neutrality the unambiguous law of the land. The commission’s ruling found that ISPs could not block consumers from accessing online content – but it did not squarely address the underlying issue of discrimination that stopped short of blocking.

Following the commission’s order, Comcast stopped its peer-to-peer blocking practices and instituted a new network management system that does not discriminate against or in favor of any Internet applications.⁸ Comcast’s new system identifies neighborhoods that are growing substantially congested,

DEEP PACKET INSPECTION: THE END OF THE INTERNET AS WE KNOW IT

and then identifies individual users within those neighborhoods that are using a substantial amount of bandwidth, and slows down those heavy users for a short period of time.⁹ Although imperfect,¹⁰ Comcast has adopted a non-discriminatory network management regime that deals with congestion without attempting to pick winners and losers on the Internet.

NEBUAD AND INTERNET MONITORING

The dangers of DPI are not limited to violations of Net Neutrality; they extend to violations of privacy as well. Until its reorganization in 2008, a company called NebuAd offered an advertising service to network providers. With this service, NebuAd devices would secretly sit at key places within the network and monitor all consumer communications passing through the network, using DPI to search within packets for URLs and search terms. The devices would then analyze some or all of that traffic to identify consumer behavior patterns.¹¹ But NebuAd's activities went beyond information gathering. NebuAd artificially inserted packets of data into the stream of traffic to redirect Web browsers to a NebuAd-owned domain for the purpose of placing unsolicited tracking cookies on the user's computer.¹²

In March 2008, Internet users began detecting unsolicited cookies originating from NebuAd systems put in place by ISPs without notice.¹³ In May 2008, NebuAd made headlines by announcing a targeted advertising partnership with Charter Communications.¹⁴ After substantial pressure from public interest groups, subcommittees from both the House¹⁵ and the Senate¹⁶ held hearings to investigate the arrangement and NebuAd's practices. As a result of intense negative feedback from Congress and its customers, Charter terminated its arrangement with NebuAd in June 2008.¹⁷ The company has now virtually disappeared, but the enticing business of consumer tracking remains an attractive proposition for many ISPs.

In the cases of Comcast and NebuAd, consumer interests won the battle, though the war is far from over. The manufacturers of DPI equipment are committed to selling tools for network monitoring and discrimination, and were not deterred by the Comcast and NebuAd debacles. The debate over the use of DPI has only begun. Appropriate uses of DPI technologies do exist. But the applications we have seen thus far are not encouraging, and the burden of proof for their benefit rests squarely with the network operator.

THE PRESENT DAY: PRIORITIZATION ON THE INTERNET

COX COMMUNICATIONS

Despite the examples of Comcast and NebuAd, other providers are instituting discriminatory network management practices. The most high-profile of these is Cox Communications. Cox operates a cable network, which by design shares bandwidth among a large number of users. When the network becomes congested at peak usage times, the user experience suffers. Cable operators therefore have an incentive to figure out a way to manage traffic to ease the congestion by discouraging bandwidth-intensive uses of the network – thus avoiding further investment in physical network upgrades. In the short term, practices that target specific uses or users may well improve consumer experiences. But in the long term, these management practices may hurt innovation in high-bandwidth applications, reduce consumer choice and shackle the free market of Internet content and services.

Cox is currently engaging in trials of a new network management system that uses DPI to identify traffic from various Internet applications, and then chooses which applications deserve high priority and which can be slowed down. Cox has not deployed these systems across its network, but is currently testing them on subscribers in Kansas and Arkansas. Cox may be well-intentioned in trying to ensure that a congested network still performs well for users. But questions remain as to why the provider opted for this system rather than adopting the network management practices publicly disclosed by Comcast after the FCC decision. In contrast to Cox's system, Comcast's current network management practices slow down all traffic from high-bandwidth users, rather than traffic from specific high-bandwidth applications.¹⁸

If extended to a network-wide practice, Cox's network management system would set an alarming precedent that a service provider may choose how different applications are treated. This practice takes away user choice and threatens to diminish the innovation at the edges that has long made the Internet valuable. Although Cox may not choose to use that power for commercial purposes, business models designed to take advantage of discrimination will emerge. These future ramifications should be seriously considered in analysis of the Cox tests or of any other company in pursuit of similar activities.

QUEUING WINNERS AND LOSERS

Prioritization in the Cox system is performed through traffic queuing. Queuing is normal behavior on the Internet – every modern router has a queue. Ordinary network operation queues packets for a second or two during bursts of usage to maintain smooth and fast traffic flow. Default queues on the Internet operate under what is known as the “best efforts” model: The router forwards the packets at the front of the queue as fast as it can; if the queue is overwhelmed, some packets are lost. This is why the Internet is sometimes referred to as a “best efforts” network.

Although the full details have not been publicly disclosed, based on Cox's initial statements, Cox's new system splits the normal queue into two queues: “less time-sensitive” or low-priority traffic and “time-sensitive” or high-priority traffic.¹⁹ The system identifies the application from which the traffic originates through the use of DPI technology. It then selects a queue based on the time sensitivity

of the application, as determined by Cox. The system sends the traffic from the low-priority queue through the router less frequently than from the high-priority queue.

By placing the two types of traffic into separate queues in the router, Cox's system can speed up certain uses of the Internet at the expense of others. For example, Cox might choose to forward three packets from the low-priority queue for every seven it forwards from the high-priority queue. Another approach would be one in which the system sends any and all packets from the high-priority queue before sending any from the low-priority queue.²⁰ The result of either approach, from the user's perspective, is that some applications will work better than others. In some cases, the differences may not be perceptible – but in other cases, they would be.

Cox hopes that the delays on low-priority traffic will be minimal – on the order of milliseconds. If delays are limited to a tiny fraction of a second, the harm to the user should be minimal. However, queues any longer than a few seconds are significantly harmful to the normal operation of the Internet. Network applications generally treat packets as lost if an acknowledgement of receipt has not been received by the destination within a couple of seconds. With most applications, this causes the original sender to resend the packet. Additionally, routing protocols and devices often treat late packets as expired, and will drop them and wait for the sender to retransmit the data. If it takes too long for packets to be sent, the use of the queue will in fact generate additional congestion rather than limiting it. Cox's system can avoid a large queue delay by aggressively dropping old packets – but that also leads to retransmission of packets. The result could be both a highly inefficient network, and a frustrated user experience as a result of even longer delays.

Internet users and policymakers should monitor closely whether the trial run of this new DPI equipment produces more harm than good. Although it may reduce congestion in some circumstances and allow some applications to function better, putting some applications into a fast lane may cause other applications to work poorly or not at all. And because of packet retransmission, Cox's system may ultimately cause more congestion, rather than less. Finally, and most importantly, the user has no control over which of their applications are treated favorably and which unfavorably. Though consumers can give feedback to Cox and alert them to problems in the new system, the power to make changes will rest with Cox.

RISKS TO INNOVATION AND THE INTERNET

Cox's DPI technology marks a major shift in the operation of the Internet. Instead of consumers and application providers controlling traffic priority, the network itself makes the choice. Even assuming a perfectly innocent motive, DPI-enabled prioritization opens a Pandora's box of unintended consequences. First, moving control over content into the network destabilizes the market for applications and services by creating an artificial preference for one protocol or type of communication over others. Second, other unexpected problems may arise with user experiences under DPI-enabled prioritization because of varying uses of the same protocol or application by different users. Ultimately, if we accept the use of non-standard network management regimes that discriminate against specific applications, we risk a "balkanization" of the Internet – a world in which every ISP operates according to its own set of rules. The result would be a hodgepodge of different networks instead of one unified

DEEP PACKET INSPECTION: THE END OF THE INTERNET AS WE KNOW IT

and universal Internet, undermining the open platform and open market principles at the root of the Internet's success.

DPI-enabled prioritization puts innovation on the Internet at risk. Innovation in peer-to-peer protocols has resulted in valuable new applications and businesses – such as BitTorrent DNA, Vuze and P2P Next – based on the use of peer-to-peer for streaming video in particular. However, if all peer-to-peer traffic is labeled low priority, efforts by these companies to provide a superior video streaming experience will fail. Over time, application developers will steer clear of disfavored protocols and make services that do not run afoul of the latest network management tools. This would create an artificial pressure point in the market and misdirect innovation around barriers that have nothing to do with user choice. It also might force application providers to pay for priority access to avoid being deprioritized and to remain competitive. Finally, DPI-enabled prioritization might lead to an encryption arms race in which disfavored applications would encrypt all traffic to evade identification by DPI. Such an outcome would render the congestion-reduction purpose of DPI ineffective.

DPI-enabled prioritization also puts the user experience at risk. Consider the FTP protocol, declared by Cox to be “low priority.” One person may use FTP to upload a photo album from a recent vacation to a Web server to share with friends and family; another may use the protocol to upload real-time images of a security system. The former can fairly be considered “low priority,” but the latter cannot. The service provider, sitting in the middle of the network and using DPI to determine that the protocol in use is FTP, cannot make that distinction – only the user can. Over the Internet, the relative urgency of traffic is not best determined centrally, but by the host applications and users generating the traffic. If some traffic needs or deserves prioritized treatment, the technical standards underlying the Internet provide a way to do this, and to allow the user (rather than the network operator) to specify which traffic is important and which is not, through the use of DiffServ or IntServ. These methods have the additional advantage of not requiring the use of DPI, making the determination of priority faster and simpler.

It is easy to imagine a future when, in the pursuit of short-term benefits, network operators choose to implement dozens of different DPI tools that discriminate against certain types of applications. ISPs would apply a variety of tools based upon the particular characteristics of their networks, producing an environment in which content, services and applications function differently from ISP to ISP. Consider the example of Primus Telecommunications Canada. Primus has announced a network management system similar to Cox's, but using different classes and classifications of priority.²¹ Even if such a system seems reasonable as a response to an individual company's congestion problems, together, the varying systems of multiple ISPs would break the Internet into a collection of distinct networks. Such balkanization would place immense burdens on developers seeking to produce consistent and useful applications and services. Such an outcome would be disastrous not only for the user experience, but for all innovation and entrepreneurship on the Internet – a market that has always assumed an open platform where any application will work across the global network of networks.

Given the range and risk of harms, Internet users and policymakers alike should be wary of permitting a wide variety of DPI management tools to enter the market without scrutiny and investigation.

ZILLIONTV: THE FUTURE OF DISCRIMINATION?

Beyond the prioritization system employed by Cox, the future of discrimination on the Internet can be previewed today through ZillionTV. The ZillionTV service streams video programming over Internet access services directly to their subscribers, without the aid of any form of local storage or buffering – offering instant availability of content.²² Subscribers to ZillionTV purchase an inexpensive box (\$50), which may contain little more than an Internet port and a video decoder, and pay no subscription fees. They can then stream video programming content, for free, if they view a few minutes of advertisements per hour.²³

ZillionTV serves the same purpose as mainstream over-the-top video services such as Hulu or Netflix's on-demand technology, with one distinct difference. To support 2.7 Mbps streams without any substantial local caching while maintaining a steady, high-quality picture without glitches over current-generation broadband networks, ZillionTV requires assistance from ISPs.²⁴

As it turns out, this assistance may be substantial. For starters, the ZillionTV box will only be available for purchase through the ISP.²⁵ According to one source, the ISP must provide "dedicated bandwidth" that is "unaffected by any Net congestion that might degrade competing services."²⁶ Similarly, another report claims, "Video wouldn't actually traverse the public Internet; rather, ISP distributors would collocate VOD servers in their own facilities for optimal performance."²⁷ Another article says that the ZillionTV deal with Hollywood studios and ISPs hinges on the delivery of video through ZillionTV faster than through Hulu or BitTorrent or other competing video delivery platforms.²⁸

It may be that ZillionTV will turn out to be nothing more than an add-on to cable TV service – a video product offered over the non-Internet portion of a local network. ZillionTV might use edge caching and might be able to operate without any prioritization or DPI. But their marketing blurs the lines, suggesting that ZillionTV may be transmitted over the Internet and gain advantages through DPI. The details remain murky, but the potential problem is clear: ZillionTV could work by claiming part of the Internet for its own use, and it would do so with the willing assistance of the ISP, which would assuredly be rewarded for the effort. And, ZillionTV has at least one major ISP already lined up as a customer.²⁹

ZillionTV's analysis of its own behavior is worthy of note. ZillionTV justifies prioritization of streaming video by citing Cox's network management trial, contending that streaming video has been recognized as a service that deserves extra "help."³⁰ Notably, if ZillionTV were not traversing the Internet, it would not need the benefit of Cox's network management practices. ZillionTV has not yet officially launched its service, and some of its initial statements and reports appear contradictory. The alleged details of prioritization and established deals with ISPs have yet to be substantiated.

But if the ZillionTV business model relies on DPI-enabled prioritization, it represents the forefront of the next generation of discrimination on the Internet: carving out a portion of the once-neutral Internet for special treatment of its own traffic. And if ZillionTV succeeds over Netflix, Hulu and other competing services that operate over the "best efforts" Internet, it will have done so not because of superior technology or new ideas, but because it broke the neutrality and nondiscrimination of the Internet.

Regardless of the credibility of the system, ZillionTV's public messaging and the media attention it has garnered hint that an entire industry waits in the wings to use DPI and discrimination to transform the Internet into a mechanism to advance its business models. ZillionTV is the first of the dangers to peek out from the Pandora's box that will be opened if we allow DPI prioritization to operate unchecked.

THE FUTURE: MONITORING AND MONETIZING THROUGH DPI

Network operators and affiliated organizations seek to frame the Net Neutrality debate in terms of the need to manage congestion, to ensure that “fairness” exists among customers³¹ or to resolve emotionally charged issues like dialing 911 with a VoIP service.³² Although helpful in presenting the operators’ case to the public, these arguments disguise the true purpose of “network management,” which is to support new tools and business models based on real-time monitoring and control of Internet traffic.

These new tools and business models, including those of Comcast, NebuAd, Cox and ZillionTV, are enabled by abuses of DPI. In fact, an entire electronics industry has arisen as this technology has matured, creating equipment that is more affordable, efficient and sophisticated. These new devices have been developed and marketed for their capacity to enable ISPs to monitor and monetize the Internet.

DPI technology itself need not be anti-consumer if it is used to resolve congestion or security problems without harmful discrimination. But the value of DPI as marketed by prominent vendors derives instead from real-time monitoring and control of the Internet, uses that are explicitly contrary to the principles of an open Internet and to consumer choice.

MARKETING DPI TO INTERNET SERVICE PROVIDERS

Marketing for DPI equipment extends well beyond private conversations with ISPs about the powers and pitfalls of the technology. Publicly available marketing materials and statements by manufacturers reveal that these devices are designed for ISPs to develop new methods to charge for individual uses of the Internet. Consider Andrew Harries, CEO of Zeugma Systems, a DPI equipment manufacturer: “Our view is that our customers’ most pressing concern is how to insert themselves into the over-the-top value chain,” he says.³³ Harries’ vision is to “enable our customers to see, manage and monetize individual flows to individual subscribers” – for example, “to deliver video quality over the Net, to either a PC or a TV, that convinces consumers to pay a little extra to the broadband service provider.”³⁴

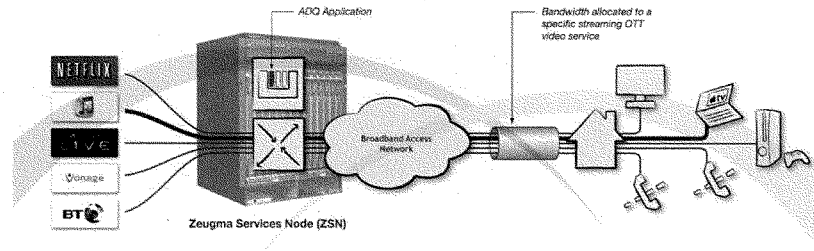
A *Telephony Online* article describes Zeugma this way:

Zeugma enables service providers to sell QoS [Quality of Service] to content delivery networks such as Akamai, insert customer-specific advertising into content for advertisers, charge consumers for certain content and also get a percentage of sales from digital storefronts, as those increase over a higher performing network.³⁵

This elaborate marketing scheme is far from hypothetical. Zeugma partnered with Netflix and Roku to demonstrate how Zeugma technology could guarantee Netflix movies reach customers faster than other movie services. In one article, a Roku representative said a deal like this “gives broadband service providers an additional product that they can use to increase per-subscriber revenue.”³⁶ At the same time, the article observes, it “remains to be seen how consumers will react to paying extra for bandwidth they can already use now.”³⁷ Network operators seem keen on exploring DPI’s potential

DEEP PACKET INSPECTION: THE END OF THE INTERNET AS WE KNOW IT

to generate new sources of revenue. Prior to launching in May 2008, Zeugma had already established trials with two North American Tier-1 providers.³⁸



Source: Zeugma, <http://www.zeugmasystems.com/solutions/applicationdrivenqos/default.aspx>

Another DPI equipment manufacturer, Allot, published a marketing brochure touting its ability to increase ARPU (Average Revenue Per User) through "Tiered Services" and "Quota Management."³⁹ Allot claims their equipment "enables quota-based service plans that allow providers to meter and control individual use of applications and services."⁴⁰ Another Allot document states:

The platform delivers high performance, reliability, application awareness and subscriber awareness, which are key components for implementing solutions to control infrastructure and operating costs, and for deploying value added services to increase total and per-subscriber revenues (ARPU).⁴¹

Allot created a tool that "enables service providers to project potential revenues and profits from setting up a tiered service infrastructure."⁴² Even more blatantly, one of the "Service Provider Needs" listed by the company is to "reduce the performance of applications with negative influence on revenues (e.g. competitive VoIP services)."⁴³

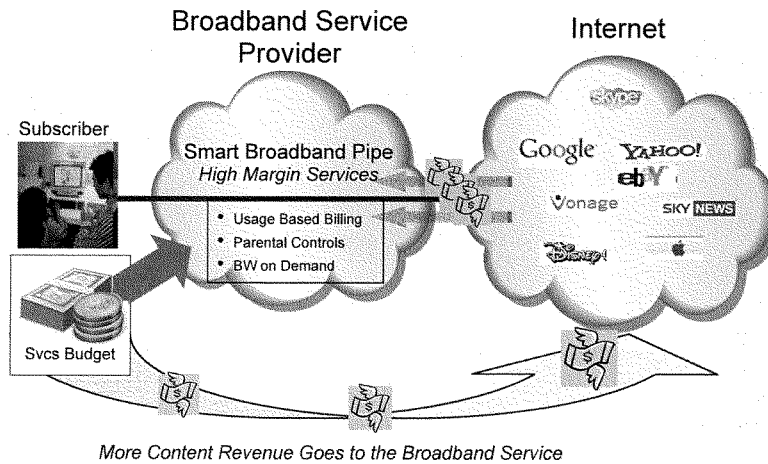
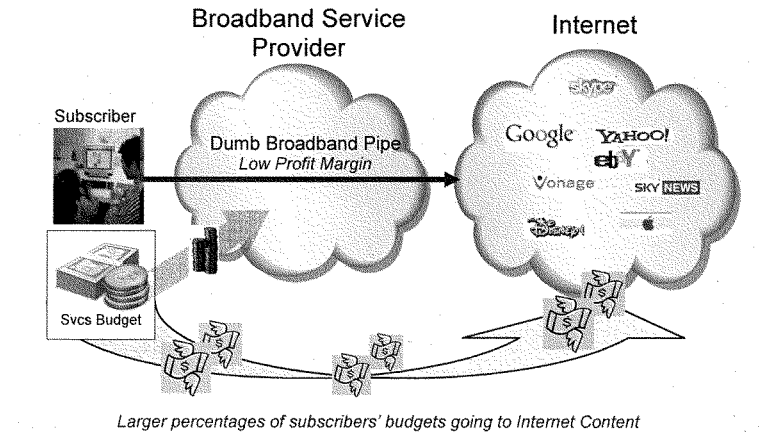
Service Provider Needs
Have an accurate view of content and applications and who is using them
Improve the performance of applications with positive influence on revenues (e.g. churn reduction)
Reduce the performance of applications with negative influence on revenues (e.g. competitive VoIP services)
Manage ever-increasing volumes and types of traffic on the network

Source: Allot Communications, <http://www.sysob.com/download/AllotServiceGateway.pdf>

Camiant, another equipment manufacturer, similarly characterizes their "Multimedia Policy Engine" as "an intelligent platform for applying operator-defined business rules that determine which customers, tiers and/or applications receive bandwidth priority, at what charge and how much they may use."⁴⁴

DEEP PACKET INSPECTION: THE END OF THE INTERNET AS WE KNOW IT

The firm's marketing has been effective – Camiant claims its DPI equipment “now reaches more than 70 percent of North American cable modem subscribers.”⁴⁵



Source: Network Strategy Partners, <http://0299d3f.netsohost.com/NewPages/DPI.pdf>

DEEP PACKET INSPECTION: THE END OF THE INTERNET AS WE KNOW IT

Openet, whose clients include AT&T and Verizon, makes a similar value proposition to carriers:

In an era when subscriber acquisition rates are declining, the focus of service providers is on increasing profitability and competitiveness, which are largely dependent upon gaining visibility into and control over the events and transactions on their networks. In fact, network activity is a valuable resource that can be exploited to produce measurable business value by the savvy service providers that have the expertise and technology to extract that value from it.⁴⁶

Along these same lines, DPI firm Procera Networks markets a brochure titled, "If You Can See It, You Can Monetize It."⁴⁷ Procera recently boasted they had added 120 new customers in the second half of 2008.⁴⁸



Source: Procera, http://www.proceranetworks.com/images/documents/procera_brochure_web_0620.pdf

The latest DPI assessment from the industry publication *Light Reading* parrots the device manufacturers' claims: "Most important, [DPI] technology also offers service providers new ways of monetizing the traffic on their networks."⁴⁹ Similarly, Cisco Systems writes, "[B]y identifying services that might be riding an operator's network for free, a provider can truly differentiate its own 'branded' VoIP service traffic from best-effort traffic or extend QoS guarantees to that third party for a share of the profits."⁵⁰

DPI SHORTCHANGES CONSUMERS

Network providers can and will use DPI technology to improve their profits at the expense of their customers. The technology permits network operators to reduce the amount they spend on network upgrades by allowing them to oversell their networks while simultaneously increasing the amount the average customer pays, through the creation of new revenue streams.⁵¹ Or, in marketing language, providers want to "deliver customized service plans that increase customer satisfaction and reduce churn."⁵²

Yes, DPI can help alleviate problems of congestion in a network, thus improving the user experience. But the same DPI technology – the same electronics equipment, in fact – also allows providers to monitor and monetize every use of the Internet, and DPI vendors succeed by developing and marketing this capability. These DPI systems may already be installed in some operators' networks. A Yankee Group analyst asserts that U.S. ISPs are currently deploying advanced DPI equipment, although

UNDER ATTACK: IN VIOLATION THE END OF THE INTERNET AS WE KNOW IT

many do not disclose it publicly.⁵³ Through these secret arrangements, the DPI industry is experiencing remarkable growth.⁵⁴

Precedent, motivation and capability all exist for providers of wireline and wireless Internet services to discriminate in the transmission of Internet content in search of new revenue streams. DPI now offers capabilities far beyond simply protecting Internet users from harm, and the service providers purchasing and installing DPI equipment are well aware of these possibilities.

If service providers flip the switch and turn on these control mechanisms, it might mean the end of the Internet as we know it.

ENDNOTES

- 1 47 U.S.C. § 202(a) ("It shall be unlawful for any common carrier to make any unjust or unreasonable discrimination in charges, practices, classifications, regulations, facilities, or services for or in connection with like communications service....").
- 2 See generally *FCC Classifies Cable Modem Service as "Information Service"*, March 14, 2002, available at http://www.fcc.gov/Bureaus/Cable/News_Releases/2002/nrcb0201.html; *FCC Eliminates Mandated Sharing Requirement on Incumbents' Wireline Broadband Internet Services*, Aug. 5, 2005, available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-260433A1.pdf.
- 3 *Appropriate Framework for Broadband Access to the Internet over Wireline Facilities; Review of Regulatory Requirements for Incumbent LEC Broadband Telecommunications Services; Computer III Further Remand Proceedings: Bell Operating Company Provision of Enhanced Services; 1998 Biennial Regulatory Review—Review of Computer III and ONA Safeguards and Requirements; Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities; Internet Over Cable Declaratory Ruling; Appropriate Regulatory Treatment for Broadband Access to the Internet Over Cable Facilities*, CC Docket Nos. 02-33, 01-337, 98-10, 95-20, GN Docket No. 00-185, CS Docket No. 02-52, Policy Statement, 20 FCC Rcd 14986 (2005) (*Internet Policy Statement*).
- 4 See *Comments of Free Press, et al., In the Matters of Free Press et al. Petition for Declaratory Ruling that Degrading an Internet Application Violates the FCC's Internet Policy Statement and Does Not Meet an Exception for Reasonable Network Management; Broadband Industry Practices*, WC Docket No. 07-52 (Feb. 13, 2008), p. 29-34, Appendix 2, available at http://www.freepress.net/files/fp_et_al_comcast_petition_fp_comments.pdf.
- 5 See e.g., Jonathan Krim, "Executive Wants to Charge for Web Speed," *Washington Post* (Dec. 1, 2005), available at <http://www.washingtonpost.com/wp-dyn/content/article/2005/11/30/AR2005113002109.html>; Paul Kapustka, "Verizon Says Google, Microsoft Should Pay for Internet Apps," *InformationWeek* (Jan. 5, 2006), available at <http://www.informationweek.com/news/showArticle.jhtml?articleID=175801854>.
- 6 *Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications*, Free Press and Public Knowledge (Nov. 1, 2007), available at http://www.freepress.net/files/fp_pk_comcast_complaint.pdf; see also *Appropriate Framework for Broadband Access to the Internet over Wireline Facilities; Review of Regulatory Requirements for Incumbent LEC Broadband Telecommunications Services; Computer III Further Remand Proceedings: Bell Operating Company Provision of Enhanced Services; 1998 Biennial Review—Review of Computer III and ONA Safeguards and Requirements; Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities; Internet Over Cable Declaratory Ruling; Appropriate Regulatory Treatment for Broadband Access to the Internet Over Cable Facilities; Broadband Industry Practices*, CC Docket Nos. 02-33, 01-337, 95-20, 98-10, GN Docket No. 00-185, CS Docket No. 02-52, WC Docket No. 07-52, *Petition for Declaratory Ruling of Free Press, Public Knowledge, Media Access Project, Consumer Federation of America, Consumers Union, Information Society Project at Yale Law School, Professor Charles Nesson, Co-Director of the Berkman Center for Internet & Society, Harvard Law School, Professor Barbara van Schewick, Center for Internet & Society, Stanford Law School* (Nov. 1, 2007) (*Free Press Petition*), available at http://www.freepress.net/files/fp_et_al_nn_declaratory_ruling.pdf.
- 7 *In re Formal Complaint of Free Press & Public Knowledge Against Comcast Corp. for Secretly Degrading Peer-to-Peer Applications; Broadband Industry Practices; Petition of Free Press et al. for Declaratory Ruling That Degrading an Internet Application Violates the FCC's Internet Policy Statement & Does Not Meet an Exception for "Reasonable Network Management"*, WC Docket No. 07-52, Memorandum Opinion and Order, FCC 08-183 (Aug. 20, 2008) (*Comcast Order*).
- 8 See e.g., Comcast Corporation, *Description of Planned Network Management Practices*, available at http://downloads.comcast.net/docs/Attachment_B_Future_Practices.pdf.
- 9 *Id.* at p. 11.
- 10 See *Letter from Ben Scott, Policy Director, Free Press to Marlene H. Dortch, Secretary, Federal Communications Commission*, File No. EB-08-IH-1518, WC Docket No. 07-52 (Oct. 14, 2008), available at http://fjallfoss.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6520175587.
- 11 See e.g., Ryan Singel, "Report: NebuAd Forges Packets, Violates Net Standards," *Wired* (June 18, 2008), at <http://blog.wired.com/27bstroke6/2008/06/nebuad-forges-g.html>.

DEEP PACKET INSPECTION: THE END OF THE INTERNET AS WE KNOW IT

- 12 See Robb Topolski, Chief Technology Consultant, Free Press and Public Knowledge, *NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking* (June 18, 2008), at http://www.freepress.net/files/NebuAd_Report.pdf.
- 13 *Id.* at 4.
- 14 "Charter hires NebuAd to make online ads more relevant," *IAB SmartBrief* (May 16, 2008), available at <http://www.smartbrief.com/news/iab/storyDetails.jsp?issueid=65693081-BF7F-4D7B-B0C4-B58D314EF624©id=75FCE22C-C5ED-4E05-B582-ED3970114D94&imcid=>.
- 15 See e.g., Grant Gross, "Lawmakers Call on NebuAd to Change Privacy Notification," *PCWorld* (July 17, 2008), at http://www.pcworld.com/businesscenter/article/148555/lawmakers_call_on_nebuad_to_change_privacy_notification.html.
- 16 See e.g., Nate Anderson, "NebuAD CEO Defends Web Tracking, Tells Congress It's Legal," *Ars Technica* (July 9, 2008), at <http://arstechnica.com/news/ars/post/20080709-nebuad-ceo-defends-web-tracking-tells-congress-its-legal.html> ("Dorgan noted that neither he nor most consumers 'have the foggiest idea' about what's being tracked, how long it's maintained, and what it's being used for").
- 17 Steven Musil, "Charter Drops Controversial Customer Tracking Plan," *CNET* (June 24, 2008), at http://news.cnet.com/8301-10784_3-9976893-7.html?tag=nfd.top.
- 18 See generally Comcast, *Frequently Asked Questions about Network Management*, available at <http://help.comcast.net/content/faq/Frequently-Asked-Questions-about-Network-Management> ("The new technique does not manage congestion based on the online activities, protocols or applications a customer uses, rather it only focuses on the heaviest users in real time, so the periods of congestion could be very fleeting and sporadic").
- 19 See generally Cox Communications, *Congestion Management FAQs*, available at <http://www.cox.com/policy/congestionmanagement/>.
- 20 Though Cox claims to be able to maintain a lower bound on bandwidth for low-priority traffic, thus making this specific example unlikely.
- 21 "Primus Introduces New Internet Traffic Shaping System," *Digital Home* (March 18, 2009), available at <http://www.digitalhome.ca/content/view/3509/280/>.
- 22 Press Release, ZillionTV, *ZillionTV Corporation Unveils First-of-Its-Kind Television Service That Delivers on the Promise of Personalized TV* (March 4, 2009), available at <http://finance.yahoo.com/news/ZillionTV-Corporation-Unveils-bw-14538971.html>.
- 23 Eliot Van Buskirk, "ZillionTV: Hollywood and ISPs Unite to Deliver Video over the Net," *Wired* (March 4, 2009), at <http://blog.wired.com/business/2009/03/one-factor-that.html>.
- 24 Nate Anderson, "ZillionTV tempts net neutrality gods with prioritized video," *Ars Technica* (March 8, 2009), at <http://arstechnica.com/tech-policy/news/2009/03/zilliontv-tempts-net-neutrality-gods-with-prioritized-video.ars>.
- 25 Buskirk, *supra* note 23 ("This service's affiliation to ISPs is so strong, you won't be able to purchase a box anywhere but through your ISP, for a one-time activation fee of \$50").
- 26 John Murrell, "Zillion? That's the eventual total of set-top box choices, right?," *Good Morning Silicon Valley* (Mar. 4, 2009), at <http://blogs.siliconvalley.com/gmsv/2009/03/zillion-thats-the-eventual-total-of-set-top-box-choices-right.html>.
- 27 Todd Spangler, "Look Like a Zillion Bucks?," *Multichannel News* (March 9, 2009), available at http://www.multichannel.com/article/189623-Look_Like_a_Zillion_Bucks_.php?rssid=20059.
- 28 Buskirk, *supra* note 23 ("Part of ZillionTV's partnership with both ISPs and Hollywood studios involves the ISPs delivering ZillionTV signals at higher speeds than those at which they deliver content from, say, Hulu or bit torrent, with whom they apparently have no such deal").
- 29 Carol Wilson, "ZillionTV Creates a New On-Demand Video Option," *Telephony Online* (March 4, 2009), at http://telephonyonline.com/video/news/zillionTV_free_video_030409/?smte=wl.
- 30 Buskirk, *supra* note 23 ("A couple of weeks ago, the Cox cable company put out an announcement regarding the matrix by which they're going to deal with those situations where their pipes are clogged," said [ZillionTV CEO Mitch] Berman. "It was a priority matrix of what they're going to do, and who they're going to help first. The first ones they say they're going to help are streaming, which is what we do.").

DEEP PACKET INSPECTION: THE END OF THE INTERNET AS WE KNOW IT

- 31 See e.g., Comments of National Cable & Telecommunications Association, *In the Matters of Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications*, File No. EB-08-IH-1518; Broadband Industry Practices, WC Docket No. 07-52, p. 3-5.
- 32 See e.g., Stephanie Condon, "Chamber Backs Broadband Deployment—without Net Neutrality Laws," *CNET* (Dec. 22, 2008), available at http://news.cnet.com/8301-13578_3-10128169-38.html; Grant Gross, "Net Neutrality Opponents Cite e-Health Efforts," *IDG News Service*, Aug. 15, 2007, available at http://www.pcworld.com/article/135949/net_neutrality_opponents_cite_ehealth_efforts.html.
- 33 Carol Wilson, "TelcoTV: Zeugma, Roku Team on Enhanced Net Video," *Telephony Online* (Nov. 13, 2008), available at <http://telephonyonline.com/iptv/news/enhanced-net-video-1113/>.
- 34 *Id.*
- 35 Carol Wilson, "Zeugma Aims to Redefine Edge," *Telephony Online* (May 27, 2008), at <http://telephonyonline.com/broadband/news/zeugma-redefine-edge-0527/index.html>.
- 36 Bob Wallace, "TelcoTV: Zeugma, Roku Demo QoE for Pay-Extra Services," *xchange*, available at <http://www.xchangemag.com/hotnews/zeugma-roku-demo-qoe-for-pay-extra-services.html>.
- 37 *Id.*
- 38 Wilson, *supra* note 35.
- 39 Allot Communications, *Subscriber Management Platform*, available at <http://www.ipnetworks-inc.com/pdfs/allot/Allot%20SMP%20Datasheet.pdf>.
- 40 *Id.*
- 41 Allot Communications, *Service Gateway*, available at http://www.cv-data.com/pdf/Service_Gateway.pdf.
- 42 Carol Wilson, "DPI Gets ROI Tool," *Light Reading* (Oct. 22, 2007), available at http://telephonyonline.com/broadband/technology/dpi_allot_yankee_102207/index.html.
- 43 Allot Communications, *Pushing the DPI Envelope* (June 2007), available at <http://www.sysob.com/download/AllotServiceGateway.pdf>.
- 44 Camiant, *Policy Server*, available at <http://www.camiant.com/products2.shtml>.
- 45 Camiant, *Camiant's PCMM-Qualified Policy Server Marks Major Milestone; Achieves over 70% Market Penetration* (Jan. 27, 2009), available at <http://www.camiant.com/press/p012709.shtml>. Camiant's customers include Comcast and Cox Communications. See Camiant, *Vodafone Hungary Deploys Camiant's Multimedia Policy Engine* (Jan. 21, 2009), available at <http://www.camiant.com/press/p012109.shtml>.
- 46 Openet, *Extracting Business Value at the Network Edge*, available at http://img.en25.com/Web/Openet/WP_Extracting_Business_Value_US_1008.pdf.
- 47 Procera Networks, *If You Can See It, You Can Monetize It*, available at http://www.proceranetworks.com/images/documents/procera_brochure_web_0620.pdf.
- 48 Procera Networks, *Explosive Adoption of Procera's PL10000 Platform* (Jan. 27, 2009), available at <http://www.proceranetworks.com/recent-press-releases/570-explosive-adoption-of-proceras-pl10000-platform.html>.
- 49 Simon Sherrington, "Deep Packet Inspection: Coming Soon to a Network Near You," *Light Reading* (Dec. 11, 2008), available at http://www.lightreading.com/document.asp?doc_id=169218.
- 50 Cisco Systems, *Deploying Premium Services Using Cisco Service Control Technology*, available at http://www.cisco.com/en/US/prod/collateral/ps7045/ps6129/ps6133/ps6150/prod_brochure0900aecd8025258e.pdf.
- 51 See e.g., Cloudshield Technologies, *Cloudshield Subscriber Services Manager*, available at http://www.cloudshield.com/applications/cs_ssm.asp ("By shaping traffic at the subscriber-level, bandwidth is made available for new revenue generating services. Rate limiting traffic allows network infrastructure build-out to be deferred, thereby reducing capital expenditures."); Arbor Networks, *Reduce Network Costs by Optimizing Bandwidth Utilization*, available at http://www.arbornetworks.com/index.php?option=com_docman&task=doc_download&gid=377 ("The ROI in the eSeries solution is achieved through cost reductions from reduced bandwidth purchases, deferred network infrastructure upgrades and improved customer support, plus new revenue associated with new service offerings").

- 52 Arbor Networks, *Arbor e100*, at <http://www.arbornetworks.com/en/arbor-ellacoya-e100.html>.
- 53 Wilson, *supra* note 42; see also Carol Wilson, "DPI: A Scorned Technology That's Thriving," *Light Reading* (July 21, 2008), available at <http://telephonyonline.com/iptv/news/dpi-scorned-but-thriving-0721/>.
- 54 Sherrington, *supra* note 49; see also Simon Sherrington, "The Greening of DPI," *Light Reading* (Nov. 19, 2007), available at http://www.lightreading.com/document.asp?doc_id=139389.

Mr. BOUCHER. Thank you, Mr. Scott.
Mr. Knapp.

STATEMENT OF BRIAN R. KNAPP

Mr. KNAPP. Good morning, Chairman Boucher, nice to see you again, Ranking Member Stearns and members of the subcommittee.

My name is Brian Knapp, Chief Operating Officer. I have responsibility at Loopt for day-to-day business operations, as well as privacy policy, data security matters and legal affairs.

Since you may not be familiar with my company, Loopt, please allow me to tell you a little bit about our company. We are a location-based service that can change the way friends and family connect, share and explore in the mobile environment. Loopt facilitates real world interactions by helping users connect on the go and navigate their social and family lives. Loopt users can see their friends and family where they are located and what is going on around them via detailed interactive maps on their mobile phones. And users can also share location information and updates with their networks of friends on a variety of popular social networks and communities. Over one million users have already registered for Loopt, and by all accounts, consumers are very excited about emerging mobile services and location services like Loopt.

Loopt itself got started back in 2005 when Sam Altman, a sophomore computer science major at Stanford University had an epiphany as he walked out of class, realizing that it would be great if he could open his mobile phone and see a map of where all his friends were. Since 2005, Loopt has grown. We are located in Mountain View, proud to be in Congresswoman Eshoo's district. We have grown to over 40 employees and our service is launched across multiple wireless carriers and mobile devices.

Today we are available on AT&T Mobility, Sprint Nextel, Boost Mobile, MetroPCS, T-Mobile and Verizon Wireless networks, as well as popular devices such as the Apple iPhone, Blackberry, and Google's Android G1. Depending on the service provider and the device, the cost of Loopt ranges from free and advertising-supported to \$3.99 per month.

From its inception, Loopt's founders and investors made a commitment to the development of strong privacy practices and policies. I began working with the company in late 2005 and was hired full-time by the company as chief privacy officer and general counsel two years ago, and they asked me specifically to focus on these areas as we developed our service and grew the company. At that time, we only had 13 other employees and we were alive on one network operator at the time. However, even in our early days, we knew that investing in an effective privacy program was necessary for our users and an important foundation for our future business growth and success.

Our privacy approach is based on the key principles of user-control, education and notice and our regime specifically includes informed consent. Our service is 100 percent permission-based, so users are choosing to download and access Loopt. We receive this informed consent from every user. They must proceed through a multi-step registration process which has key information about

how the service works and how they should use it responsibly. And there are several ways to access our key user agreements and privacy policies. At the end of my testimony there is actually a flow chart of this process that you can see.

We have reminders and notifications even after users have registered to again have them keep in mind how to use the service responsibly and access the privacy settings. Speaking of privacy settings, we have several controls so they can manage where, when, and with whom their location is shared and displayed.

Also, any friend connections or family connections made on Loopt are also chosen by the user so there is no automatic sharing of location information. You have to decide who you are going to share that information with and then you can still control it after the fact.

We also have age limits on our service so our minimum age is 14 years and we have implemented an age-neutral screening mechanism in compliance that works in accordance with the FTC's guidance with regard to COPPA best practices. We have report abuse links throughout the service so the community can give us feedback if other users seem to be behaving badly. Our privacy notice and user education are key aspects of our regime. Our privacy notice is readily available and viewable within the mobile application itself and on our Web site and may actually be received by e-mail or postal delivery for our users. Our Web site contains detailed information about our privacy features, as well as frequently asked questions, and there are several links on the homepage of that site to access this information.

I want to emphasize that we have developed these policies by listening to our customers and working closely with leading mobile social networking and online privacy and security organizations, including the Center for Democracy and Technology, the Electronic Frontier Foundation, the Family Online Safety Institute and Progress and Freedom Foundation, among others.

We also participated in an Internet safety technical task force and finally, we also participated in the development of CTIA's Guidelines and Best Practices for Location-Based Services. And our accomplishments to date in terms of privacy and security innovation would not have been possible without the great feedback, insights and know-how of these organizations and folks on the hill.

We believe that the result of all this collaboration is a consistent, sound set of privacy policies that apply to all of our users, regardless of where they live or use the service. We know that Loopt's customers value their privacy and especially the easy access to tools and information to control their privacy settings as needed so we have created a privacy policy and regime that is both straightforward, effective and easy to understand. We do note that this is an evolutionary process.

We look forward to participating in these hearing and learning from other companies and the hill. And we will continue to strive for excellence in privacy innovation and aspire as a company to achieve effective privacy by design.

Thank you for the opportunity to share our story, and I look forward to any questions you may have.

[The prepared statement of Mr. Knapp follows:]

TESTIMONY OF MR. BRIAN KNAPP
CHIEF OPERATING OFFICER
LOOPT, INC.

BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES COMMITTEE
ON ENERGY & COMMERCE
SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY & THE INTERNET
HEARING ON COMMUNICATIONS NETWORKS AND CONSUMER PRIVACY

April 23, 2009

Good morning Mr. Chairman and Members of the Subcommittee, my name is Brian Knapp, Chief Operating Officer at Loopt with responsibility for day-to-day business operations as well as privacy, policy, data security matters, and legal affairs.

Since you may not be familiar with Loopt, please allow let me tell you a little about our company.

Loopt is a location-based service that changes the way friends and family connect, share, and explore in the mobile environment. Loopt facilitates real-world interaction by helping users connect on the go and navigate their social lives. Loopt users can see where their friends are located and what's going on around them via detailed, interactive maps on their mobile phones. Users can also choose to share location information and updates with their network of friends on a variety of popular social networks and communities.

Over 1 million users have registered for Loopt. By all accounts, consumers are very excited about emerging mobile services like Loopt.

We got started back in 2005 when Sam Altman, a sophomore computer science major at Stanford, had an epiphany as he walked out of class – realizing that it would be great if he could open his mobile phone and see a map of where all his friends were.

Since 2005, Loopt has grown to over forty employees and our service has launched across multiple wireless carriers and mobile devices. Today, Loopt is available on AT&T Mobility, Sprint Nextel, Boost Mobile, MetroPCS, T-Mobile, and Verizon Wireless networks as well as popular devices such as the Apple iPhone, RIM Blackberry, and Google's Android G1. Depending on the service provider and device, the cost of the Loopt service ranges from free ad-supported to \$3.99 per month.

From its inception, Loopt's founders and investors made a commitment to the development of strong privacy practices and policies. I began working with Loopt in late-2005 as outside counsel, and was hired full-time by the company two years ago to specifically focus on privacy, policy, and data security. At the time, Loopt had 13 other employees and only one operator partner, Boost Mobile; however, even in our early days we knew that investing in an effective privacy program was necessary for our users and an important foundation for our future business growth and success.

Loopt's privacy approach is based on the key principles of user-control, education, and notice. Our regime specifically includes:

- Informed Consent. The Loopt service is 100% permission-based; express, informed opt-in consent is received from every user. Each user must proceed through a multi-step registration process, during which they are presented with key information about the service and several ways to review Loopt's end user agreements. At the end of my testimony is a flow diagram illustrating this process.
- Reminder Notification Program. Following registration, an automated notification program reminds users that Loopt is now installed on their mobile device, and contains key messages about how to best manage their privacy on the service.
- Location-Sharing End User Controls. Loopt users completely control where, when, and with whom their location is shared or displayed, and all Loopt "friendship connections" are reciprocal and may be removed or deleted at any time. Loopt users may "hide" their location at any time or even set a fixed location (non-GPS) manually. Users share location information only with their

in terms of privacy and security innovation would not have been possible without the great feedback, insights, and know how of these organizations.

We believe that the result of all this collaboration is a consistent, sound set of privacy policies that apply to all of our users, regardless of where they live or use the service. Consumers' privacy expectations don't change when they cross geo-political boundaries. This is an important point for policymakers to consider in a world that is becoming increasingly mobile-centric.

We know that Loopt's customers value their privacy and especially the easy access to tools and information to control their privacy settings as needed. In response, we have created a privacy policy that is both straightforward and easy to understand. This is an evolutionary process and we will continue to strive for excellence in privacy innovation and aspire as a company to achieve effective "privacy by design".

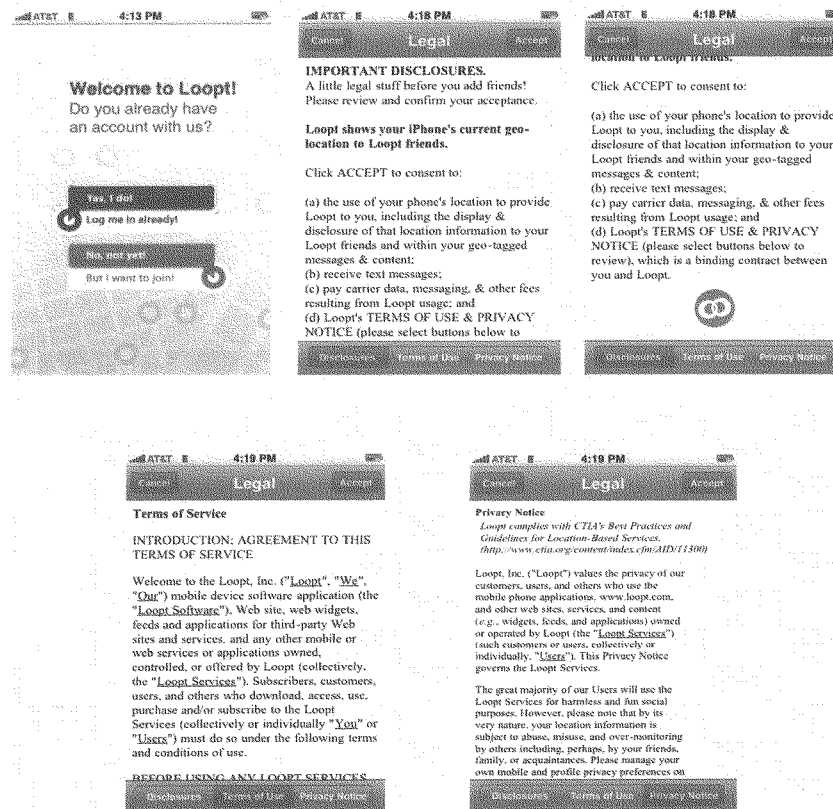
I thank you for the opportunity to share Loopt's story with the Subcommittee, and I would be pleased to answer any questions you may have.

selected friends, networks, and services. Loopt users can easily turn location-sharing on or off at any time on a friend-by-friend basis or for all friends at once.

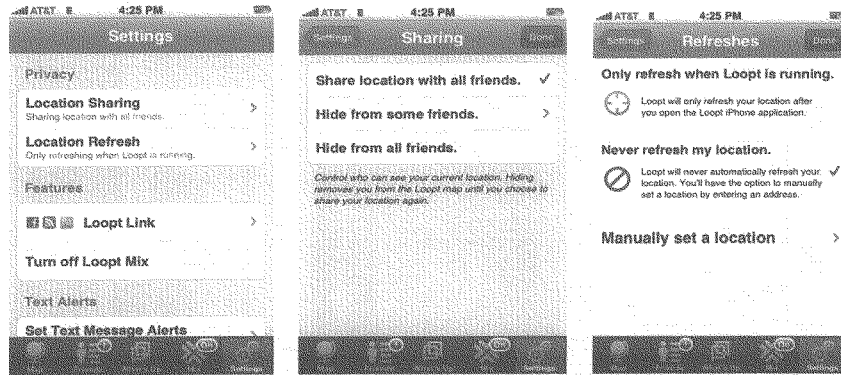
- Age Limits. Loopt's Terms of Use includes a minimum age requirement, currently set at 14 years of age. Loopt has implemented an "age-neutral" screening mechanism in its user registration flow, which requires – in a neutral fashion – users to input their age and rejects users who do not meet the minimum requirement. Loopt tags the mobile device of such unsuccessful registrants and prevents those prospective members from re-registering from the same device. This screening mechanism works in accordance with the FTC's guidance with regard to COPPA best practices. In addition, parents and guardians may contact Loopt at any time to terminate accounts of underage users.
- Report Abuse. "Report Abuse" links are posted near every user profile. Loopt's customer service and privacy-response team reviews all Report Abuse messages and responds appropriately according to internal process standards and Loopt's Terms of Use. Loopt will promptly notify, suspend, or permanently ban users who violate Loopt's community policies and regulations including the posting of inappropriate content or the harassment of other users.
- Privacy Notice, User Education. Loopt's Privacy Notice is readily viewable within our mobile application and at Loopt.com, and may be received by email delivery or postal mail. Loopt is TRUSTe certified. In addition, Loopt's Web site contains detailed information about our privacy features as well as frequently-asked-questions.

We developed these policies by listening to our customers and working closely with leading mobile, social networking, and online privacy and security organizations such as the Center for Democracy & Technology, Electronic Frontier Foundation, Family Online Safety Institute, Cyber Safe California, ConnectSafely.org, Congressional Internet Caucus Advisory Committee, and the Progress & Freedom Foundation's Center for Digital Media Freedom. Loopt was also a participating member on the Internet Safety Task Force, originally formed by MySpace and 49 States Attorney Generals, and managed by Berkman Center at Harvard University. Finally, we were active participants in the creation of the CTIA's Guidelines and Best Practices for Location-Based Services. Our accomplishments to date

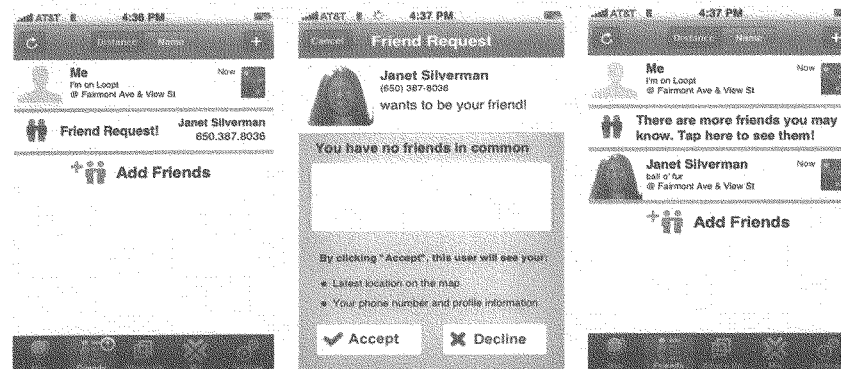
Loopt – Informed Consent / Opt-In. The following screenshots from Loopt's iPhone application illustrate the user consents, sign-up flow:




Loopt Location Privacy Settings:



Making Loopt "friend connections":



Privacy Policies. Links to Loopt's privacy policies and related tips and frequently-asked-questions are prominently placed on the Loopt Web site home page:



[The Service](#)
[What Is Loopt?](#)
[Partners & Products](#)
[Privacy & Security](#)
[The Company](#)
[An Overview](#)
[Our History](#)
[Executives](#)
[Board of Directors](#)
[Useful Links](#)
[Our Blog](#)
[Stay Loopt In!](#)
[Loopt in the News](#)
[Jobs at Loopt](#)

[Privacy & Security](#)
[Jump to: Privacy Features](#) [For Parents](#) [Be Safe](#)
[Login](#)
[Sign Up](#)

Privacy Innovation

Privacy and security are key company priorities at Loopt. We strive for excellence in privacy innovation and aspire to achieving effective "privacy by design". Loopt offers the most intuitive and effective privacy controls and security features for end users. Questions? Comments? Let us know! privacy@loopt.com

Loopt is 100 percent permission-based and users share location information only with their selected friends, networks, and services. Loopt users can easily turn location-sharing on or off at any time on a friend-by-friend basis or for all friends at once.

Loopt works regularly with select organizations that focus on privacy & security including: [The Family Online Safety Institute](#) (board member), [ConnectSafety.org](#), [PewResearch.org](#), [Electronic Frontier Foundation](#), [National Network to End Domestic Violence](#), [Progress & Freedom Foundation's Center for Digital Media Freedom](#), [Internet Education Foundation](#), and [Cyber Safe California](#) by the [California Office of Privacy Protection](#) (member, advisory committee). Further, Loopt sits on the [CTIA's WTC Leadership Council](#) and was an active participant in the creation of the [CTIA L&E Best Practices](#).

Loopt is also a participating member on the [Internet Safety Task Force](#), originally formed by [NCSpace](#) and all [State Attorney Generals](#), and now managed by [Berkestan Center](#) at [Harvard University](#).

Public speaking & community participation regarding privacy & security:

- Participant: [Progress & Freedom Foundation's Aspen Summit](#), "Data, Media & Marketing" roundtable
- Panelist: [Family Online Safety Institute](#), invitation-only roundtable, "Searching for Online Safety Solutions"
- Panelist: [Family Online Safety Institute](#), Annual Conference '07
- Exhibitor: State of [Net '08](#) by [Advisory Committee to Congressional Internet Caucus](#)
- Panelist: [2008 Cyber Safe California](#) by [California Office of Privacy Protection](#)

Loopt Buzz

Apr 16th, 2009
Wall Street Journal
Andy Jordan's Tech Diary:
Online Hookups Get Geo-Aware.
 People are using location-based social networking to meet strangers online, in their own neighborhoods, spontaneously and in real-time. WSJ's Andy Jordan takes a look at Loopt. [read more...](#)

Apr 14th, 2009
GPO Business News
Eric Carr, Loopt: "we are definitely north of 1 million users"
[Eric Carr, Vice President of](#) [see all news](#)

Mr. BOUCHER. Thank you, Mr. Knapp.
Mr. Bennett.

STATEMENT OF RICHARD BENNETT

Mr. BENNETT. Good morning, Mr. Chairman, Mr. Stearns and members.

Thanks very much for inviting me. This is the first Congressional meeting I have actually attended in person since Senate Watergate. So maybe I should tell you what I know and when I came to know it.

I am actually—some said there are no technical experts here. I am kind of offended by that because I am supposed to be one. I have been developing network systems for some 30 years in the Ethernet and Wi-Fi systems that use today include some innovations that I personally invented and put there. And so when I look at these technologies the sort of collection of technologies that are coming under the umbrella of deep packet inspection, I think I have a slightly different perspective on it than most people do because what I see them as is an evolution of the tools that we have used to develop network technologies over the years.

It has been essential in the development of every network protocol and in every network access device to have intelligence about the behavior of the systems that are communicating and the forwarding behavior of the intermediate nodes and the network that move the packets along. Without the ability to have that information we would not have been able to develop the systems that we all use today on the Internet and on the related private networks that feed the Internet.

We never called this deep packet inspection. We simply called it packet monitoring and that process which was largely a matter of running a system that had filters that could capture packets from a live network and store them for the immediate examination and analysis by a network engineer, has been automated into a system that takes that information that has always been accessible to network engineers. There is not any—I mean I take issue with Mr. Scott that there has been some new leap forward in this technology in the last year. I mean there really hasn't. It is a smooth evolution from the systems that we have always used for manual analysis into archiving and data-mining, and these are the features that have actually changed in the use of this technology over the years.

The raw information has always been there and the raw information is there because digital networks typically don't carry encrypted traffic. And the reason for that is a lot of the information that you might think of as payload is actually header from another point of view as Mr. McSlarrow indicated. When we examine a network packet there is in fact a series of headers that you get that you have to go through before you get to final payload. And there is no actual location in that packet where you can draw a bright line and say everything to the right of this is payload, everything to the rest is header because applications invent protocols on top of protocols, on top of protocols and it is a more or less never-ending process because that is how new services are born on the web.

So I am not worried about the use of deep packet inspection if I can use that term for network management purposes. For net-

work management purposes it is vitally important for network operators to be able to apply network engineering principles, not for the purpose of making competing services perform less well but to make them perform more well.

In one of the reasons that Comcast implemented the system that they got in so much trouble for a couple of years ago was because they had customer complaints that Vonage was not working well on their network. And they analyzed the traffic on their network to troubleshoot this problem that customers were reporting with Vonage's voiceover IP service and what they found was the rise of peer-to-peer traffic was causing delays for Vonage. And this is because peer-to-peer traffic puts enormous volume on the uplink side of a network that was engineered primarily to supply data in the downlink direction. And the reason it is engineered that way is because that simply is the way that data flows on the worldwide web and when you click on a Web site you send a small message upstream and what you receive downstream is, you know, 30, 50, 100,000 bytes.

So the networks are engineered to behave asymmetrically. A new application comes along that actually puts more data on the uplink side then it draws down on the downlink side and it destabilizes the network engineering throughout the entire network. And so the engineering tools are applied to identify that problem and they made a crude attempt and they admit—I mean I am actually more positive about their attempts than they are. They admitted that their attempt to resolve that problem was done incorrectly and so the way that that should be done is in a more anonymous and more protocol-neutral manner where they simply collect data about the volume of traffic that individual users are putting on the network over a 15 minute period of time. So this is a beneficial use.

In my written testimony, there is a little footnote where I try explain why I think the issue of deep packet inspection is so—there is so much animosity against it. Now, I think what is actually behind that is a dispute over two competing regulatory models for advanced telecommunication services like Internet and broadband. The traditional method has been described by FCC Commissioner McDowell as technology silos, where we regulate telecom one way. We regulate information services another way and every new technology that comes along becomes the subject of a new raft of regulations. Well, it turns out that technology silos approach with Title One, Title Two regulations isn't effective when you have competing services like voice and video that can be delivered across different platforms. And so there are a couple of different ways to address that problem and one solution that has been proposed is to go to a functional layering model where the different layers of the network are regulated according to different standards.

So we treat carriers one way because that they are basically moving packets across a network. We treat web services providers a different way because they are on top of that infrastructure. But I think that approach which essentially is just rotating the silos model 90 degrees to the right exhibits a lot of the same problems because what you have is the ambiguity of services. E-mail is a service that can be provided by an ISP and traditionally is but it can also be provided by a web company like Google or Yahoo. Is

there some reason why Google and Yahoo's e-mail should be regulated differently from an ISP's e-mail? I don't think there is. E-mail is e-mail is e-mail. It is a service.

Mr. BOUCHER. Mr. Bennett, you are now about 2½ minutes over your time if you would wrap up.

Mr. BENNETT. I am sorry. I got too inspired.

Mr. BOUCHER. That is quite all right.

Mr. BENNETT. So that is my pitch is that I think that rather than focusing on the technology, it makes more sense to look at the services themselves and to begin with the standards of proper disclosure and truth in advertising that any service should have.

[The prepared statement of Mr. Bennett follows:]

Richard Bennett
661 Ruby Rd.
Livermore, CA 94550

April 21, 2009

The Honorable Chairman Rick Boucher
The Honorable Ranking Member Cliff Stearns
The Honorable Chairman Henry A. Waxman
The Honorable Ranking Member Joe Barton
The Honorable Members of the Subcommittee on Communications, Technology, and the Internet

Subject: Testimony before the House Committee on Energy and Commerce Subcommittee on Communications, Technology, and the Internet hearing on April 23, 2009

Dear Chairman Boucher, Ranking Member Stearns, and members of the Subcommittee,

Thank you for offering me the opportunity to address the subcommittee on the subject of technologies that monitor consumer use of communications networks. The topic is pertinent to the evolution of the networks, to the development of consumer awareness, as well as to potential new regulations if they're needed. I'd like to offer a few recommendations.

Network Monitors

I'm a network engineer, inventor, and writer. I've designed data transfer and Quality of Service protocols for some of our most widely used communications networks, switched Ethernet and Wi-Fi, as well as for some that haven't got off the ground yet, such as Ultrawideband. As a consequence I've had occasion to use a variety of network monitoring and analysis equipment to observe traffic on networks.

Network monitors – often called “Sniffers” after a popular product produced by Network General in the 1980s – enable engineers to see every part of the packets that traverse the network segments to which the monitors are attached, including the various payloads present at the Ethernet, IP, TCP, HTTP, and Content layers, for example. These are vital tools that permit programmers and electrical engineers to accelerate systems and isolate and correct bugs that would otherwise limit network function. These systems pre-date the Internet by many years, and it's safe to say that we would have no working packet networks without them.

These devices have political uses as well – the controversy over Comcast's first-generation traffic shaping system was set off by a network technician who used an open source network monitor to discover suspicious TCP packets mingled in amongst the peer-to-peer file sharing packets he expected to see. Since the 1980s, these devices have had the ability to apply filters to network traffic based on sophisticated pattern matching, to produce logs of selected packets, and to perform a variety of statistical analyses to network traffic streams. They are frequently used by network administrators to troubleshoot problems in both local and wide-area networks, and are generally considered to be invaluable aids in maintaining the semblance of stability that users expect of their networks.

While these monitors have been used on occasion to steal passwords and other user information, these instances are rare and limited in scope simply because an Ethernet monitor can only be used to capture traffic on the particular part of the network to which it is attached. If I monitor the

traffic on my home network, as I frequently do, I can't see any of the traffic generated by my neighbors, even though we share a common coaxial cable to a shared CMTS; this is because my cable modem only passes traffic intended for my Internet access account. The only clue I have to my neighbors' usage is the delays that my traffic encounters on the way up and down the cable, and that only tells me how busy they are, not what sites they're visiting and which files they're downloading.

To obtain that level of information, I would have to use a Wi-Fi sniffer such as Air Pcap and hope their Wi-Fi networks are either completely unsecured or that they rely on an effectively useless cipher such as the deprecated *Wired Equivalent Privacy* standard known as WEP.

Anyone who uses a Wi-Fi network in a populated area without securing it with WPA or WPA2 is effectively sharing his personal web surfing and e-mail habits with any snoop who cares to hear them. This situation is intolerable to me, so I joined colleagues in the Wi-Fi Alliance in developing a system for quick and easy setup of secure Wi-Fi networks called Wireless Protected Setup or WPS. I hope all of you who use Wi-Fi understand that you're broadcasting your web surfing habits to anyone who cares to learn them if you haven't secured your networks. If you're forced to use an unsecured Wi-Fi network in exigent circumstances, you can provide yourself a measure of privacy by securing your e-mail connection with Transport Layer Security. Public Ethernet connections are also fundamentally insecure, as anyone connected to the same switch fabric you're connected to can easily capture your packets and examine them to his heart's content.

As a purely technical matter, there's no difference between the means that Wi-Fi engineers use to diagnose network problems and those used by snoopers on public Wi-Fi networks to steal passwords: the same packet capture tool can do both. But one activity is legitimate (and even necessary to the proper functioning of networks) and the other is not.

So my first recommendation to the committee is to **emphasize intent and behavior rather than technology** in its continuing efforts to protect communication privacy. Technologies are neither good nor bad, it's the uses we put them to that matter.

The Culture of Over-Sharing

Another threat to consumer privacy, and in my mind a much greater one, is what I'll call the Culture of Over-Sharing. With the advent of personal web sites, blogs, social networks, and Twitter, people are sharing information about themselves that would certainly make their grandparents blush. I follow a number of tech journalists on Twitter, and I can now tell you more details of their personal health, diets, and dating habits than about the stories they cover or the conferences they attend. I don't particularly care for this personal information, but it's a part of the package.

Stories abound about young people who've posted drunken party pictures of themselves while they were in college finding embarrassment, often costly, when they apply for jobs and have to explain their antics to Google-savvy recruiters. The Internet is a harsh mistress, and much of what happens there stays there, seemingly forever.

I've been operating a series of blogs on technology and politics since 1995, and recently have received a number of requests from past commenters to remove missives they posted to a blog a few years ago. One recent correspondent said his roommate had posted radical sentiment under his name (I have no way to verify one way or another,) and another admitted frankly to being

young, reckless, and grammatically challenged when posting comments that he now feels make him less employable. So I've adopted a policy of removing older comments for any reason at all. The lesson that I draw from this is that **retention policies are critically important to privacy**. It's the nature of networks to disseminate information, public and otherwise, but the game doesn't change radically until past, present, and future are combined into large, searchable archives that holds us captive to our pasts forever. People, especially those who were young once, need to have the ability to reinvent themselves, and our culture of over-sharing combined with our massive Internet archives, is eroding it.

Consumer Education

I've alluded to consumer awareness, or the lack thereof already, but I'd like to emphasize it as there have been recent instances of inadvertent sharing. CNet News reports¹ that the Committee on Oversight has heard testimony on the following events:

- On February 28, 2009, a television station in Pittsburgh reported that the blueprints and avionics package for "Marine One," the President's helicopter, was made available on a P2P network by a defense contractor in Maryland.
- On February 26, 2009, the Today Show broadcast a segment on inadvertent P2P file sharing, reporting that social security numbers, more than 150,000 tax returns, 25,800 student loan applications, and nearly 626,000 credit reports were easily accessible on a P2P network.
- On February 23, 2009, a Dartmouth College professor published a paper reporting that over a two-week period he was able to search a P2P network and uncover tens of thousands of medical files containing names, addresses, and Social Security numbers for patients seeking treatment for conditions such as AIDS, cancer, and mental health problems
- On July 9, 2008, the Washington Post reported that an employee of an investment firm who allegedly used Lime Wire to trade music or movies inadvertently exposed the names, dates of birth, and social security numbers of about 2,000 of the firm's clients, including Supreme Court Justice Stephen Breyer. There have been reports alleging file sharing programs have been used for illegal purposes, such as to steal others' identities.

Technology always moves faster than regulation, and we want to keep it that way, but consumers need to be aware that some of the applications they run, particularly peer-to-peer file sharing applications, expose more information than they may want. It's unlikely that producers of Peer-to-Peer applications will be responsive to Congressional mandates of full disclosure; theirs is a quirky community with little regard for authority, but steps can be taken to make consumers aware of the dangers of inadvertent over-sharing.

Malware and Botnets

Perhaps the most significant threat to consumer privacy is deliberate identity theft. By now, this threat is well-understood: millions of computers worldwide are infected with viruses that put them under the effective control of the virus' creators. Infected computers, tied together in a huge *botnet*, are used to send Spam and to run key-loggers that steal personal information. The end

¹ Greg Sandoval, "Congress to Probe P2P Sites over Inadvertent Sharing," *CNet News*, April 21, 2009: http://news.cnet.com/8301-1023_3-10224080-93.html?part=1&subj=news&tag=2547-1_3-0-20

produce is sent back to the controller where it's used for criminal purposes. It's suspected that some botnets may be controlled by foreign intelligence services as they're shown up in interesting places, such as the Dalai Lama of Tibet's offices in India. While Spam is in integral part of the Internet's e-mail system today, and will remain so as long as we don't adopt a system of user authentication as part of normal e-mail practice, efforts to mitigate its effects are impressive.

Spam fighters maintain a set of DNS Blacklists which squelch, by their estimation, some 81% of attempted Spam at the source, simply by checking the Internet Domain Name of the source networks against a list of known Spam networks. This is a very important function, but it raises the shackles of some privacy advocates, who see it as discriminatory and non-transparent. DNS Blacklists certainly do contain false positives from time to time, but they incorporate procedures for the removal of domains unfairly listed. The value of this kind of Spam mitigation is enormous, and it goes beyond the protection of consumer privacy: Spam has a considerable carbon footprint and contributes to global warming. According to a recent report by McAfee, Inc²:

- *An estimated worldwide total of 62 trillion spam emails were sent in 2008*
- *The average spam email causes emissions equivalent to 0.3 grams of carbon dioxide(CO2) per message*
- *Globally, annual spam energy use totals 33 billion kilowatt-hours (kWh), or 33 terawatt hours (TWh). That's equivalent to the electricity used in 2.4 million homes, with the same GHG emissions as 3.1 million passenger cars using two billion U.S. gallons of gasoline.*
- *Spam filtering saves 135 TWh of electricity per year. That's equivalent to 13 million cars off the road*
- *Much of the energy consumption associated with spam (nearly 80 percent) comes from end users deleting spam and searching for legitimate email (false positives). Spam filtering accounts for just 16 percent of spam-related energy use.*

Clearly, Spam mitigation is a social good. The Blacklist method isn't sufficient on its own; it's driven by intelligence about which e-mail messages are Spam and which aren't. This determination is made by a number of means, one of them human intelligence, but machines are part of the process as well. Mechanical recognition of Spam depends on a process of pattern matching e-mail against known contents of Spam currently in circulation in the Internet. Like anti-virus software, Spam detectors search for Spam signatures in ordinary e-mail, flagging or deleting suspect messages. This is in fact a very invasive process, one that can often cause legitimate messages to end up in user's spam folder or worse. But it's a system that Internet users embrace because its benefits far outweigh its drawbacks.

The lesson I suggest we should learn from Spam mitigation is to **examine mechanical processes for their practical benefits as well as their theoretical harm** to abstract notions of privacy, and to consider what our networking experience would be like without them. The damage to personal privacy inflicted by Spam signature searches has to be balanced against the greater harm that unchecked Spam inflicts. Similarly, an e-mail ethos based on personal identity rather than semi-anonymous access has benefits that are not lost on the architects of Internet e-mail. Future systems will surely be designed in more robust manner.

² *The Carbon Footprint of Email Spam Report*. McAfee Inc. and ICF International, http://img.en25.com/Web/McAfee/CarbonFootprint_28pg_web_REV.PDF, retrieved April 21, 2009.

Traffic Engineering

Contrary to popular belief, the physical networks that carry Internet Protocol packets are not “stupid” networks. Most IP networks of significant size carry a combination of generic Internet traffic and private IP traffic that has to be delivered according to Service Level Agreements (SLAs) between end-user organizations and network carriers. Some SLAs are very stringent, allowing for as little as 2 milliseconds of latency (delay) between transmitter and receiver. In order to satisfy the needs of customers with varying SLAs, network operators buy network equipment that’s capable of prioritizing packets. These systems depend on the ability to classify network flows³ and to count packets per second over long periods of time. Their prioritization function interacts with accounting and policy functions to promote or demote specific flows depending on the customers standing in terms of volume and rate and his contract. Traffic engineering of this sort, generally using the MPLS⁴ protocol which reduces the overhead of repetitive route lookup as the packet moves from one router to another, is at the heart of the modern Internet.

A simplified form of traffic engineering is now employed by Comcast on its residential broadband network to protect IP service from overload. When a link has been congested for a meaningful period of time, the system identifies heavy users of network resources (bandwidth.) Any of these users who’ve exceeded a meaningful threshold are placed in a lower priority category until the load they offer the network declines. This system is notably “protocol agnostic” as it treats all Internet applications the same: if a user is engaged in a large file transfer for a significant period of time (15 minutes or more) that places him in the low priority category, and if the user is also using Skype or some other VoIP service, his VoIP performance will suffer until he takes steps to curtail his downloading.

This system addresses one of the fundamental architectural shortcomings of the Internet, the absence of a per-user fairness system. This problem has been addressed in numerous forms, and perhaps most clearly by Dr. Bob Briscoe, Chief Scientist at British Telecom Research⁵:

Resource allocation and accountability keep reappearing on every list of requirements for the Internet architecture. The reason we never resolve these issues is a broken idea of what the problem is. The applied research and standards communities are using completely unrealistic and impractical fairness criteria. The resulting mechanisms don't even allocate the right thing and they don't allocate it between the right entities. We explain as bluntly as we can that thinking about fairness mechanisms like TCP in terms of sharing out flow rates has no intellectual heritage from any concept of fairness in philosophy or social science, or indeed real life. Comparing flow rates should never again be used for claims of fairness in production networks. Instead, we should judge fairness mechanisms on how they share out the 'cost' of each user's actions on others.

The Internet is a system built on the dynamic sharing of network bandwidth, but it lacks a general-purpose mechanism of allocating it across user accounts fairly. Because the Internet lacks this vital mechanism, it’s necessary for network operators to supply it themselves, as they have since the first deployment of Internet Protocol in a wide-area network by Ford Aerospace in 1981.

³ A “flow” is a series of packets between a common source and destination.

⁴ E. Rosen, A. Viswanathan, and R. Callon, *Multiprotocol Label Switching Architecture*, January 2001, IETF RFC 3031, <http://tools.ietf.org/html/rfc3031>

⁵ Bob Briscoe, *Flow-Rate Fairness Dismantling a Religion*, http://www.cs.ucl.ac.uk/staff/B.Briscoe/projects/2020comms/refb/fair_ccr.pdf

While the network engineering community is acutely aware of the limitations of the Internet's architecture and protocol design, advocates for open access and related causes often gloss over this issue in their search for the perfect network. The network technician who discovered the original Comcast system for managing P2P by injecting TCP Reset packets complained that the user-volume-based system amounted to "discrimination based on user-history [sic]."⁶ If that's the case, it's a brief history, no more than 15 minutes long.

The lesson to be learned about traffic engineering is that the realities of business and the shortcomings of the Internet as a global system for multiple uses often collide with utopian desires for the more perfect network. In very real sense, the TCP/IP Internet remains a work in progress 35 years after it was proposed as a research network for the exclusive use of highly-trained network engineers, professors, and graduate students. It was somewhat unfortunate that it was pressed into service in a completely different role in the early 90s when the plethora of personal computers demanded interconnection. Compromises against ideals of network function are inevitable in this scenario, and should not automatically be judged failures simply because they violate abstract notions of network design that have never been more than pipe dreams.

Standards bodies continue to address the Internet's need for continual improvement, and researchers are hard at work on several projects that would replace the current Internet with an improved network that reflects some of the knowledge we've gained in the last 35 years. In the meantime, I would urge the Committee **not to hold Internet operators to unrealistic standards**. Keeping the Internet running smoothly is a difficult task in the best of times, and any practice that has a plausible connection with this goal should be seen as constructive and responsible, even if it requires accounting for usage and acting accordingly. In the long run, traffic management systems that rely on accounting and prioritization are much friendlier to innovation than those that simply charge for usage.

Deep Packet Inspection

Discussions like this one inevitably come to Deep-Packet Inspection, that poorly-defined term that seems to portend something ominous ("it was a dark and stormy night for IP packets.")⁷ As I've endeavored to show, there are legitimate and illegitimate uses for most aspects of network technology, and this is no exception. If we recognize that much of the traffic on the Internet is digital piracy (it doesn't matter how much as long as we agree that it's significant,) we have to accept that some means of mitigation is appropriate, just as it is for Spam, viruses, and overload. The most effective means of piracy mitigation – other than jail time for the operators of piracy-enabling web sites and tracker services like The Pirate Bay – is a system in which piracy cops enter swarms of users downloading and sharing digital material in a manner contrary to law. This system doesn't rely on DPI, as it simply uses non-encrypted information made available by the

⁶ Robb Topolski, *Re: [p2pi] Follow-Up from Comcast Presentation*, e-mail to IETF P2PI, June 6, 2008. <http://www.ietf.org/mail-archive/web/p2pi/current/msg00072.html>

⁷ A great deal of the animosity against DPI seems to stem from the belief that a functional layering approach to communications regulation should replace the current model, which FCC Commissioner McDowell has described as "technology silos." The silo model is defective because it focuses on technologies rather than services, and breaks down in the face of the similarity between video, IP transport, and voice services delivered across multiple technologies. Unfortunately, the functional layering model simply rotates the silo 90 degrees, and retains multiple ambiguities due to the fact that networks often perform similar functions – such as retransmission and error detection – at multiple layers. The service and disclosure model currently used by the UK telecom regulator, Ofcom, is far superior to either.

pirates, perhaps inadvertently. Encryption doesn't make this any harder to do, as the fabric of P2P piracy is sharing known content with random partners across a network. These exchanges revolve around a content identifier known as a file "hash" which is computed across the entire range of a file. File hashes can be extracted from certain P2P transactions automatically, and these transactions can point the piracy cop toward trackers who may not have been known at the outset. Hence, DPI has a role, albeit a limited one, in piracy mitigation. As long as digital piracy is against the law, there has to be some accepted means of finding it and stopping it. This needn't involve door-to-door searches or trips to Guantanamo Bay, but it's not simply a matter of sitting on our hands and saying, as the founders of The Pirate Bay said after their conviction in a Swedish court, that anything easy to do should be legal⁸.

DPI can also be useful as a means of relaxing per-user quotas imposed by a fairness system, to better tune network service to application requirements. In a more perfect Internet – the one envisioned by the architect of the IP datagram's Type of Service field, the architects of Integrated Services, and the designers of Differentiated Services – applications should be able to communicate requirements to the network, and the network should do its best to meet them according to the service level that a user has purchased. It's for this reason that the Internet Protocol's header structure includes a field for signaling such requirements to the network. Unfortunately, in the transition from research to production network, this signaling was overlooked. Moving the Internet off the NSF Backbone and onto a mesh of private networks required the invention of a new protocol for service providers to communicate routing information with each other. This protocol – Border Gateway Protocol (BGP) – did not include a mechanism for attaching Quality of Service levels to routes. Private IP networks overcome this problem by adopting MPLS and using Ethernet VLANs, but the problem of communicating QoS levels in the public Internet remains unresolved. There is hope that a draft pending before the IETF's Inter-Domain Routing Working Group provides the solution⁹. The creator, a professor at the Chemnitz University of Technology, has tested his solution in number of public Internet exchanges in Europe and reserved the necessary numbers from ICANN.

In the meantime, the most effective way of determining application requirements is to examine streams and map them to QoS categories by their evident properties. Generally speaking, networks can provide the greatest utility if they can expend their most scarce resource, low-latency delivery, on the packets most in need of it. In the consumer scenario, these are VoIP packets. VoIP is a low-bandwidth application, generally requiring no more than 128 kilobits/second, and often much less. It's a stringent application in terms of delay, however, as it can't tolerate latencies greater than 150 milliseconds (thousands of seconds) from end to end. VoIP is generally recognized as a candidate for a network boost. P2P file sharing, on the other hand, is a candidate for demotion because it tends to use as much bandwidth as is available, and to do so for a very long time, often in the range of hours. Once an ISP has determined stream requirements, it can adjust its handling so as to provide rapid delivery for VoIP and economical delivery for P2P. This is simply a matter of assigning packets to appropriate SLAs within and without the ISP's network. If every interconnected part of the Internet doesn't immediately support such an extension of past functionality, there's no cause for alarm as some day most will. The intersection of technology, economics, and marketing is too compelling for any other outcome.

⁸ Owen Thomas, "Jail Time Shuts Down The Pirate Bay Joke Machine," *Valleywag*, Apr 17 2009. <http://gawker.com/5216499/jail-time-shuts-down-the-pirate-bay-joke-machine>

⁹ Thomas Martin Knoll, Simple Inter-AS CoS, March 9, 2009. <http://www.ietf.org/proceedings/09mar/slides/idr-5.pdf>

So there's no reason to fear the use of DPI for traffic engineering. There is no loss of personal privacy from such behavior, nor would its adoption drive the Internet into a posture that's less friendly to competition. If anything, **the ability of applications to select a transport service appropriate to their needs would be an enormous boon to developers** of either time-sensitive or volume-sensitive applications. They only suffer if all traffic has to be treated as if it were the same when it's clearly different.

Tracking Cookies

One development that concerns me is the expanded use of tracking cookies to build dossiers of user behavior across the Internet. The most notorious current example is the Double-Click DART cookie¹⁰ used by Google's AdSense program. The DART is a unique identifier placed in a user's computer by Google to track his or her movements around web sites that participate in the AdSense contextual advertising program. DART cookies as currently conceived are not especially evil – they simply allow advertisers to know how many times users have seen their ads on average, and which web sites are frequented by the same people - but there's something creepy about writing a blog post critical of Google and knowing that everyone who reads it essentially reports as much to the mother ship. Although the DART identifier is simply a random number with no particular connection to a discernable human being, the portion of the Internet's population who have both Gmail accounts and DART cookies certainly are potentially identifiable to anyone with sufficient access to Google's data base.

The prospect of ever-increasing dossiers of Internet users with information about who they are, where live, who their friends are, what blogs they read, and what trips they take is simply disturbing. While there is no evidence that this tracking data has yet been abused, it's simply a matter of time until a deranged Googler tracks an ex-girlfriend or an over-ambitious product manager applies some artificial intelligence to predict what we will buy that we didn't even know we wanted.

I have no particular recommendation regarding tracking cookies and the related dossiers but for the Committee to keep an eye on the way they're used and on the lookout for feature creep. All collectors of information seem to share the attitude that if a little bit of information is good, a lot is better, and all information tends to leak over time.

Conclusion

The most effective means of monitoring consumer behavior is a well-placed virus, and failing that it's a system of web tracking with a persistent cookie linked to a personal account. A number of technologies with primarily beneficial uses have been demonized for eroding privacy, often unfairly. The greatest threats to consumer privacy are not technologies – we're awash in technology – but business models that depend on the bartering of personal information. The Internet is unfortunately surrounded and permeated by an "information wants to be free" ethos in which advertising is the key source of revenue for the providers of application and content-level services. This business model inevitably collides with personal privacy concerns, and needs to be constantly monitored. I fear the only way to ensure robust protection for personal privacy in the long run is to replace the open-access, advertising-supported business model with one in which we pay for content and services. Given the strength of the Internet's now well-established tradition of pushing ads into and alongside practically everything that we see, this is not going to

¹⁰ <http://www.doubleclick.com/privacy/faq.aspx>

Bennett Testimony to House Subcommittee on Communications, Technology, and the Internet, Page 9

be an easy transition, if it's to happen at all. But as long as personal information is the coin of the realm, it will be harvested, archived, and bartered.

Thank you for your kind attention,

Richard Bennett
BroadbandPolitics.com

Mr. BOUCHER. Thank you very much, Mr. Bennett and thanks to each of our witnesses this morning for your informative testimony.

So a question that I have all of you are invited to comment on this relates to whether or not we have anyone at the present time using network technologies for behavioral advertising purposes. NebuAd has gone. Is anyone using packet inspections specifically today for the kinds of activities that NebuAd I suppose is the way you pronounce this but NebuAd was using at the time this subcommittee had a hearing on that practice during the last Congress, Mr. Rotenberg?

Mr. ROTENBERG. Mr. Chairman, my understanding is that there is no provider in the United States right now that is using DPI for targeting in large measure because of the work that was done by this committee last year. But the activity is continuing in the United Kingdom and that is very interesting to watch both by the response of the companies, some of which have said that they will not participate, and also by the response of the European commissioners responsible for privacy protection who have said they are going to try to crack down on this practice. But my understanding in the U.S. is that it is not currently taking place.

Mr. BOUCHER. Thank you. Do any of you have suggestions for other kinds of network technologies apart from the ones we focused on today and that would be specifically deep packet inspection, the new possible uses of cable set-top boxes and the GPS tracking chips that are now placed in some mobile devices? Those are the three we focused on today. Are you aware of any other similar kinds of technologies that carry significant privacy implications that we should keep an eye on, Ms. Harris?

Ms. HARRIS. Mr. Chairman, I just think it is important to clarify and maybe this is Brian's to clarify and not me that GPS is not the only way that location is being collected for services. So I think there is somewhat of a misunderstanding that GPS chips and I would rather Brian describe it then I but, you know, I wouldn't want—I would rather we focus on location services because if you say GPS then it actually will not reach a lot of the mobile services that are going.

Mr. BOUCHER. That is appropriate. Any further comment on that question, Mr. Rotenberg?

Mr. ROTENBERG. Well, this follows from Leslie Harris' point. If your concern, for example, is about mobile tracking in the network environment then I think you should also look at the issue of IP addressing. In other words, the designation that is associated with a device in the network can reveal a great deal of information about the user of the device and the location of the device. It is actually what enables services like Loopt, for example, to track users.

Mr. BOUCHER. All right. Any further comment, Mr. Knapp?

Mr. KNAPP. Yes, I mean I actually am not entirely sure about the IP address association but there are a wide variety of location technologies that enable these kind of applications consumers are enjoying. And, you know, I would just say that also speaks to why any consideration on legislation in this regard needs to be very considered so it is not sort of immediately put out of date by a new technology and broadly consider location information as you do other data.

Mr. BOUCHER. Thank you, Mr. Knapp. Ms. Attwood.

Ms. ATTWOOD. Mr. Chairman, I would like to answer the question that I would have liked you to ask me and broaden I think your intent. I think it is important to understand that the device isn't the concern that should be the focus of a privacy hearing because technology will improve and advance. I think in the USA Today story about how there is concerns about using social networks by individuals in the security context, you know, there will be advances in technology and devices. I think the question is starting from the proposition of are there things that we need to be looking at as an industry relative to protecting privacy interests and in that regard I would agree.

Mr. BOUCHER. Let me get to that in a subsequent question. I was just focusing for the moment on the presence of emerging technology. I wanted to make sure we were covering the waterfront in the terms of the technologies that we need to keep an eye on so but thank you for that. I am actually going to come to that now and I want to begin by commending both you and also Mr. McSarrow on your announced intention to protect consumer privacy in association with the use of technologies that can reveal an extensive amount of information about those consumers. My precise question to you, to both of you, is whether you have developed privacy policies to the level of detail of the application of consumer opt-in as compared to consumer opt-out. Have you gotten to that level of detail in terms of formulating and announcing your consumer protection policies?

Ms. ATTWOOD. Well, with respect to the specific topic of DPI, we have in fact announced that we will not use DPI. We don't use it today and we will not use DPI in connection with behavioral advertising without the customer's express meaningful consent.

Mr. BOUCHER. And does express meaningful consent imply opt-in?

Ms. ATTWOOD. It absolutely can imply opt-in. I am going to push all of you in the committee as we learn more about these issues to advance our thinking and our discussion about what we mean by opt-in. Opt-in is an old terminology. Opt-out is an old terminology.

Mr. BOUCHER. In our thinking, it basically means that your customer would have to take an affirmative step of some kind in order to expressly authorize you to engage in the identification and tracking process. So checking a box, clicking a box on the Web site would be an example of opt-in.

Ms. ATTWOOD. It would absolutely be an example of a customer engagement and what we have committed to is that we will in fact bring the customer into that decision about how their information is used before we use any DPI for behavioral advertising. And I think really I commend and I encourage you to look at Loopt's way in which they have approached it and they have absolutely worked on a very small form which is a mobile device and made sure that customers not only check a box but actually engage with the service provider, understand what they are purchasing and therefore get the benefit of it.

Mr. BOUCHER. So it is opt-in plus?

Ms. ATTWOOD. I would say it is engagement and it is in fact a complete transparency and customer control, yes.

Mr. BOUCHER. OK. Thank you. Mr. McSlarrow.

Mr. MCSLAW. Mr. Chairman, as an industry I don't think we have made any announcement but I can, as you suggested, report that at least for the ISPs, when you are talking about user data providing the bedrock for behavioral targeted advertising, they recognize the burden has got to be a lot heavier. It has got to approximate and I sort of associate myself with Dorothy's comment about whether it is opt-in or not but the point is that the step, affirmative step taken by the consumer after engagement and education we have recognized is the necessary precondition to moving forward.

Mr. BOUCHER. OK. Thank you. Mr. Knapp, you as Ms. Attwood has suggested, are using a form of opt-in in order to gain your customers' consent before you engage in location activities using mobile devices. What brought you to that model? What were the considerations and can you describe how that works in your application?

Mr. KNAPP. Sure and I think the illustrations in the back of my testimony are great if members would like to turn to that and sort of see the flow that the user goes through but the key is and it is with all of these applications the users are choosing to access them and so, you know, in the case of Loopt they are choosing to download it from the AT&T deck or the Apple's iPhone, the App-store. They download it and then they need to sort of set-up Loopt to work for them. And it was very clear to us that users want to be in complete control of whether a company like Loopt was accessing their location information and then allowing them to share it with others. And so it was pretty key for us given that they were going to use our application to share it with others to make sure that they initially walk through a step to set it up that educated them about the application and the service. So, you know, I mean a lot of these key privacy principles go back even a few decades to 1980 when the OECD published those and I think, you know, in subsequent privacy practices. And that is also why I mentioned before with regard to location information it is certainly sensitive information but I think you can look at and as we did other privacy laws and principles that are out there and guidelines, and apply them broadly to information like location.

Mr. BOUCHER. Thank you, Mr. Knapp. My time has expired. The gentleman from Florida, Mr. Stearns, is recognized for 5 minutes.

Mr. STEARNS. Thank you, Mr. Chairman. Mr. Rotenberg, I have had the opportunity to hear you as a panel witness particularly when I was chairman of the consumer trade and protection subcommittee. Although the bill is a little old, it was dropped in the 109th Congress, the Consumer Privacy Protection Act, HR1263, which my good friend, Mr. Boucher, was a co-sponsor. He and I worked together on this bill. Do you think that bill as it has been written could be used as a starting point for this? And how would you change it today for a general privacy bill for out of this subcommittee?

Mr. ROTENBERG. Thank you very much for the question, Mr. Stearns. I also want to commend you by the way because I do remember that series of hearings that you held on consumer privacy which I think were very important hearings. I would need to go

back and look at the legislation that you and the Chairman had put together. I do recall thinking at the time that we needed to be sure that the policies gave consumers some meaningful control over their information. That it wouldn't be enough just for the consumers to be told the policy of the company and then to consent, opt-in or opt-out, but we really wanted to give consumers the assurance that for example security standards were being followed. One of the things that we have learned over the last few years of course is that we have problems today with security breaches in the U.S. and it impacts business and the Internet user. So I think that would be important. There is always this difficult issue of course of a State preemption. I appreciate that the businesses would like a national standard. That is a tough one.

Mr. STEARNS. That was one. If you might just take a moment and go back since you are an educator and you could give us a good sounding, it might be helpful for Mr. Boucher and I to have your written comments about the bill and what you think. Is anyone else on the panel familiar with the bill that I dropped, H.R. 1263, that Mr. Boucher and I who would like to comment on it? Yes, Ms. Harris.

Ms. HARRIS. Mr. Stearns, I think we would have to go back and refresh our memory, as well.

Mr. STEARNS. OK.

Ms. HARRIS. You know, at the time I think we, you know, there were always as Marc has said, series of questions about preemption, about standard, just thinking about development since then, behavioral advertising we have to sort of put it in context but we would be glad to come back to you.

Mr. STEARNS. OK. Mr. Bennett, you had mentioned in your opening statement about in some cases the difference between an ISP services and a web-based services, you know, if you are talking about sort of web-based services like Google and Microsoft and Yahoo, do you think they should be—have a separate type of privacy policy or is the privacy policy that we apply applicable to them too?

Mr. BENNETT. I think e-mail is e-mail and it doesn't matter whether it is provided by the ISP or by a web-based services provider. I think the exact same standards for disclosure and transparency should apply to a web-based service that is equivalent like e-mail is to services traditionally been provided by ISPs.

Mr. STEARNS. To your knowledge, are the people providing e-mail today, web-based services, are they scanning our e-mails for certain words? To your knowledge, could that be?

Mr. BENNETT. Google absolutely does. I mean the web-based e-mail services are primarily advertising supported because unlike the ISPs they don't collect a subscription fee. So some of them have an option where you can get the advertising taken off your e-mail.

Mr. STEARNS. But does that prevent the web-based service from still scanning if you click that?

Mr. BENNETT. I believe it would. I can't say that for a certainty.

Mr. STEARNS. But you are saying right now that most of these web-based services are scanning our e-mail for certain words using that as a double back to give us advertising so that when I go on one of these which I do, I see all these ads and sometimes these

ads are for things that appear to me that I have just been interested in not too long ago.

Mr. BENNETT. Um-hum.

Mr. STEARNS. So if that is true, do you think that is considered something that should be part of a privacy bill so that consumers are aware when they go on their e-mail that their words are scanned, that their e-mail is being scanned?

Mr. BENNETT. I think it depends on a judgment that you have to make about consumer awareness. I mean it seems to me that people that subscribe to an e-mail service like Yahoo or Gmail are aware of the fact that it is an advertising supported service and I think Google does a pretty good job of disclosing the fact that they scan the e-mails for contextual clues so that they can put more relevant ads, you know, alongside the e-mails.

Mr. STEARNS. Yes, Mr. McSllarrow, the Chairman had mentioned the Project Canoe and it is being used I think to track consumers watching. I think you might just give us an idea what the status is of the cable industry with this Project Canoe, what it is really about and how it is being tracked and what the future is for the cable industry?

Mr. MCSLLARROW. Sure, it is now called Canoe Ventures. It is a consortium of six cable operators.

Mr. STEARNS. Can you tell us who they are?

Mr. MCSLLARROW. I should be able to remember that, Comcast, Time Warner, Brighthouse, Cablevision. I will have to get you the complete list.

Mr. STEARNS. Cox?

Mr. MCSLLARROW. I believe Cox, yes.

Mr. STEARNS. Yes, OK.

Mr. MCSLLARROW. And I know I am missing somebody. Basically the idea is to build a platform to work with program networks and advertisers to allow them to deliver more relevant advertising to the consumer. The classic example used by the CEO of Canoe Ventures is the ideal would be to make sure you could deliver a dog food commercial to a household that has dogs, in the here and now.

Mr. STEARNS. So this is an interactive operation where there must be a remote for the customer on Comcast, for example, and when this program comes up they can hit a remote which will tell them yes they want it then that is a feedback, has information that the cable operator gives to the advertiser which in turn he puts an ad back in to give.

Mr. MCSLLARROW. It could be.

Mr. STEARNS. Could be.

Mr. MCSLLARROW. Today they only have two products that they are planning on launching and one uses just third-party demographics data. It doesn't have any set-top box user data at all.

Mr. STEARNS. No interaction.

Mr. MCSLLARROW. The second one would be what you just described which would be a commercial comes up and you have an opportunity to hit a button and say yes I would like to order a pizza. So it is that built-in, opt-in system. In preparing for this hearing, I actually asked them the question whether or not they had any plans to use set-top box generated data for purposes of advertising. It is not even on the product road map but they do recog-

nize if and when down the road they get to a point in time where they would have to take a look at that, they would have to comply fully with the Cable Act which exists today and I think they are very conscious of the privacy implications of everything they do but as I said it is not even on the product roadmap.

Mr. STEARNS. All right. Thank you, Mr. Chairman.

Mr. BOUCHER. Thank you, Mr. Stearns. The gentlelady from California, Ms. Eshoo, is recognized for 5 minutes.

Ms. ESHOO. Thank you, Mr. Chairman, and thank you to each of the witnesses. This has been a really a valuable experience to listen to each of you coming at the subject matter for the subcommittee today. First, Ms. Attwood, I didn't when you talked about opt-in, does AT&T support opt-in?

Ms. ATTWOOD. AT&T for the use of DPI for behavioral targeting, yes, we have said we will not use DPI for behavioral.

Ms. ESHOO. Because you used the word engagement, you said we support engagement.

Ms. ATTWOOD. Yes, I think engagement.

Ms. ESHOO. You want to talk about weddings, we want to talk about this.

Ms. ATTWOOD. Yes, sure, I think engagement is actually a better way to describe what we are talking about which is customer awareness but—

Ms. ESHOO. So you do support opt-in?

Ms. ATTWOOD. Yes.

Ms. ESHOO. OK. Now, in the last three years AT&T, as you know, has paid more than \$21 million to resolve FCC claims that it misused a customer's personal information. What is your policy moving forward to get away from that record?

Ms. ATTWOOD. We are very proud of our record is supporting our customers' privacy. I think you are referring to UPN issues.

Ms. ESHOO. Well, \$21 million in fines is a lot. I don't know who else in the industry has paid that much and we don't want past to be prolog and so I am giving you the opportunity to tell the subcommittee where you move—how you move forward and what kind of policy AT&T would support beyond opt-in?

Ms. ATTWOOD. So part of the success story in any fine and any enforcement action is the fact that we have committed to improve our policies and in fact stand up and acknowledge the cooperation and work with the regulatory agency in order to ensure the protection of the customer information at issue there. So we absolutely pledge to continue to work on that.

Ms. ESHOO. Good. OK. Now, on I have a couple more questions. Has AT&T used AudioScience.com to place ads on the web?

Ms. ATTWOOD. Not to my knowledge if you are asking AudioScience with respect to DPI solutions, is that what you are asking?

Ms. ESHOO. Well, it is my understanding that that is the case is it?

Ms. ATTWOOD. No.

Ms. ESHOO. I mean do you—does, has AT&T used AudioScience?

Ms. ATTWOOD. We do not use a DPI solution to place ads on our web, no.

Ms. ESHOO. Does AudioScience.com notify customers when data is collected or you don't deal with them at all?

Ms. ATTWOOD. I am not familiar with the dealings with AudioScience. I am happy to get back to you with respect to that particular vendor.

Ms. ESHOO. OK. I would appreciate that. To, Mr. McSlarrow and Ms. Harris, in Mr. Bennett's written testimony he says "I fear the only way to ensure robust protection for personal privacy in the long run is to replace the open access advertising supported business model with one in which we pay for content and services." I guess this modern day "modest proposal" is one solution. I think it would destroy a free and open Internet and that it would in turn fix all of the privacy concerns that we have discussed today. But I think the real issue here is what you think or if you think that consumer privacy and a free and open Internet are compatible?

Mr. ROTENBERG. Yes, well Congresswoman I understand where Mr. Bennett is coming from. I mean there is the concern right now that if we continue down the unregulated advertising model that is sustaining the Internet, there is no stopping point. And I even raise in my testimony the related concern that this won't only be about privacy. This will be about web publishers because the content on the Web sites will become less valuable to the advertising networks as they learn more about the users. They will effectively bypass the content which will actually weaken the publishing industry. So I don't even think it is just privacy that is at risk in the unregulated advertising model. I think it is web-based publishing that is at risk, as well. Now, while I am sympathetic to his view, I do think advertising is important and can help sustain a lot of the Internet as long as limitations are established. That is really the key here. If we can say yes we need advertising. We understand that and there is a benefit here by having Internet with advertising but we are going to draw some lines and you are not going to get to do these tremendous profiles of users that are currently taking place. I think that is a sustainable model. In fact, that is the tradition in the publishing world. You know, publishing up until recently had done very well for the user, for the publisher and for the advertiser but we are going down a road right now which I am afraid will actually lead to collapse.

Ms. ESHOO. Kyle, you want to say something?

Mr. MCSLARROW. Well, I think the short answer is I think they are compatible. I think, you know, one of the great—I mean we can all, at least some of us can remember, you know, the day that the Internet was sort of commercialized but that is the world we live in and I think the great thing about the Internet is it has proven that you can take what was an old broadcast advertising model with a lot of waste and refine it in a way that allowed the services we have today. To me, the next step by keeping privacy in mind is to make that advertising model potentially even more relevant and more useful to advertisers. I just think it lists the entire Internet so I think we have to recognize privacy is an important part of it but I do think for the future of the Internet that kind of targeted advertising is going to be essential.

Ms. ESHOO. Ms. Harris.

Ms. HARRIS. Well, I remain skeptical about the value of the behavioral advertising in the long run but, you know, it is here and I think the, you know, at the end of the day it is can we get a privacy regime in place that is going to put consumers back in charge and be able to make choices.

Ms. ESHOO. I agree.

Ms. HARRIS. I think that if we are chasing each business model, each technology, we are not going to be able to do this and we have to step back and ask what is it that we want to give consumers the right to do in terms of controlling what is reasonable and put that in place.

Ms. ESHOO. And in going back to the exchange I believe that you had with the Chairman, you see that as best being carried out, implemented how?

Ms. HARRIS. Well, I think we need a law that is a privacy framework.

Ms. ESHOO. Yes.

Ms. HARRIS. That is, you know, that we move that has to do with data collection wherever it is collected and right now strong sectoral laws. We have cable law that is fairly strong. We really on the Internet except for if you make a privacy promise and fail to keep it then you have a FTC violation, you don't have any rules. We have some sectors that engage in self-regulation that is reasonably robust but that is not ultimately going to be an answer given how this is going.

Ms. ESHOO. Because it is not tameless.

Ms. HARRIS. It is not going to be enough.

Ms. ESHOO. Thank you very much.

Ms. HARRIS. Sure.

Ms. ESHOO. Thank you, Mr. Chairman.

Ms. BOUCHER. Thank you very much. Thank you, Ms. Eshoo. The gentleman from Florida is recognized for a unanimous consent request.

Mr. STEARNS. Thank you, Mr. Chairman. I just want to put the testimony of Scott Cleland, the president for Precursor, LLC. He testified before the Energy and subcommittee, our subcommittee on July 17, 2008, and I think it would be relevant to have his part of this hearing. So if you ask unanimous consent to be made a part thereof.

Mr. BOUCHER. Without objection.

[The information appears at the conclusion of the hearing.]

Mr. BOUCHER. The gentlelady from Colorado, Ms. DeGette, is recognized for 5 minutes. I am sorry, 7 minutes in total.

Ms. DEGETTE. Thank you very much. Thank you very much, Mr. Chairman. I want to follow-up on the line of questioning that Ms. Eshoo was talking about because I am concerned on the one hand I think DPI has shown to be an effective and an efficient way to deal with spam and other security issues. On the other hand, I am thinking here about consumer protection and the choices that people have to make in accessing services or Internet content. And listening to the witnesses talk about opt-in or consumer knowledge or whatever terminology you want to use about it, it really underscores for me something Ms. Attwood said which is we don't really know what we mean when we say consumer knowledge or assent.

For example, with Mr. Knapp's company, we were impressed by all the levels of informed consent that you ask for but I also have, I am sure your company doesn't do behavioral advertising. That is not what you are getting the informed consent for, correct?

Mr. KNAPP. We will support our service with advertising.

Ms. DEGETTE. Are you going to do behavioral advertising with DPI?

Mr. KNAPP. Generally no, DPI is not something that we—we are a mobile application.

Ms. DEGETTE. Right, it is a different application.

Mr. KNAPP. Exactly.

Ms. DEGETTE. So are you going to say to your consumers now we are going to monitor what we are going to use this technology to do behavioral advertising that is tailored toward you and your habits? Do you want to opt-in to that? Are you going to do that?

Mr. KNAPP. And we in fact do. We are going to support Loopt through advertising.

Ms. DEGETTE. No, that is not my question.

Mr. KNAPP. Sure.

Ms. DEGETTE. Is that going to be part of the informed consent that you give?

Mr. KNAPP. Yes.

Ms. DEGETTE. OK. Good. Now, that is admirable because my question is to Mr. McSllarrow, is that going to happen with all of the members of your association, that that is the kind of informed consent that the consumers are going to have?

Mr. MCSLLARROW. I think actually I need to back up. I represent not just ISPs but also networks and I make a distinction among them because and this is one of the points, there are many actors on the Internet. For the ISPs, yes, we recognize that there is a heavier burden to use the personally identified.

Ms. DEGETTE. So they are going to say to people, I mean they are going to say to people now if you give informed consent what that means is that your communications are going to be tracked and tailored for behavioral advertising?

Mr. MCSLLARROW. Yes, I think the notice in disclosure has to be as robust as possible. I mean this has to be legible and the English people need to understand this is exactly what we are talking about.

Ms. DEGETTE. That is great. Ms. Harris, you are nodding your head.

Ms. HARRIS. We testified in front of this subcommittee last year on behavioral advertising saying that is what is required. Frankly, we think it is required already under the Electronic Communications Privacy laws. Obviously, we want that incorporated into a Consumer Privacy law but that is the right answer. I think it is hard. I think given the fact that ISPs are in a position where they are not in daily contact with their users, you haven't made a decision to go to a site, the online environment has not done a good job yet with opt-out so I think this is a difficult step. It is a big commitment and it will be difficult to implement but it is the right choice.

Ms. DEGETTE. Right. Well, I agree with that and I am happy to hear both of you say that you are going to do that. Ms. Attwood, is that also the intention of AT&T?

Ms. ATTWOOD. Yes and we stated that on several occasions with respect to our ISP service, yes.

Ms. DEGETTE. That it would be because I think consumers now understand. I know when I sign up for some kind of Internet communication or whatever it says, you know, our policy is we do not sell or otherwise communicate your data to other people unless you check here so people get that. I am not sure they understand DPI or what that means and I am wondering, Mr. Rotenberg, is eager to address this issue.

Mr. ROTENBERG. Well, Congresswoman, I would like to join this chorus and certainly opt-in would be preferable to opt-out but I don't think it is sufficient. And I don't think it is sufficient because it won't be meaningful unless consumers actually understand what data about them is being collected and how it is being used.

Ms. DEGETTE. That is my point.

Mr. ROTENBERG. And I think the mistake that is often made is that we place so much emphasis on a policy and so much emphasis on obtaining consent that the person who is actually being asked to make the decision really doesn't have any information to make the decision. So for many of these Internet-based techniques, people really need to know what information about them is being collected. Show it to me and who are you giving it to and for what purpose? Now, if the person is OK with all of that, then you say yes, that is consent.

Ms. DEGETTE. That is exactly what I am trying to say.

Mr. ROTENBERG. OK. Well, that is great.

Ms. DEGETTE. And the reason why I am concerned about that is because I don't think that certainly people above a certain age like me, may not understand exactly how this data can be used or where it can go. People under a certain age don't have—I think of my two teenaged daughters. They may not have the sophistication to understand why that could be a problem which is why I think you have to have adequate disclosure and education.

Mr. ROTENBERG. Right and if I could say one more point because, you know, my children are on Facebook now and we spend a lot of time looking at privacy issues with Facebook. And one of the things that struck me is that young people are actually pretty sophisticated about what information they put up, what information they don't put up. And when the change of the terms of service changed for Facebook, they organized and objected and Facebook listened and there has been a very important process going on because the users of the service knew what was happening. But and here is a very important related point, the information about Facebook users that flows to advertisers and application developers, people know very little about and it is those applications that they don't have any meaningful control over.

Ms. DEGETTE. That is right and so that is why I think we really we can say informed consent or we can say consumer awareness or whatever but we need to make sure that they understand exactly where that information is going.

Mr. ROTENBERG. Yes.

Ms. DEGETTE. And I think everybody up here is shaking their heads so I think, Mr. McSlarrow, do you agree with that concept?

Mr. MCSLARROW. I totally agree with it and not only is it the right thing to do, I think it is good business.

Ms. DEGETTE. Great. OK. Thank you. Thank you very much, Mr. Chairman.

Mr. BOUCHER. Thank you, Ms. DeGette. The gentleman from Illinois, Mr. Rush, the chairman of the Subcommittee on Consumer Protection is recognized for 5 minutes.

Mr. RUSH. Thank you, Mr. Chairman. And, Mr. Chairman, I want to begin by really thanking you for your comments earlier in this hearing. I want you to know that I look forward to working very vigorously with you and on this particular issue and look forward to our joint hearing that we will be having in the near future. Mr. Chairman, I am going to start out with some questions that I would like for all of the panel if they would just even provide either a yes or no answer. And the question I am going to get right to what I believe for me is the heart of the matter, do you think that Congress should pass consumer privacy legislation with regard to all of the communications network?

Mr. ROTENBERG. How many votes do I get? Yes.

Mr. RUSH. Well, from Chicago we will see where we wind up at and then we will add something to it. OK. All right. I am beginning with you.

Ms. HARRIS. Yes, absolutely we need to develop a baseline consumer privacy bill that is based on fair information practices across all technologies. And frankly we need a bill that covers all collection and goes beyond this, you know, the media environment. We have got sectoral laws right now that hit some sectors and not others so I mean we need to do both and it is not clear to me it should be done separately. We need a baseline consumer privacy bill that has to do with data collection and obviously there is a need to reconcile the fact that we have different or no standards in media but from a consumer protection point of view, I think it is probably broader than that.

Mr. RUSH. OK. The fellow next to you.

Mr. MCSLARROW. OK. Mr. Chairman, no but I would like to be at the table when you or we do.

Mr. RUSH. OK. All right.

Mr. ROTENBERG. Yes, Mr. Chairman.

Mr. RUSH. Yes, OK.

Ms. ATTWOOD. I guess I would have to say it depends and certainly I can echo the comments that everyone has made about a broad based look. I encourage the kinds of discussions that we are having today but it may be premature and that is quite frankly so that we can get better educated and as an industry so we have an opportunity. There is a lot of complex relationships that govern this environment and in order to get a complete answer we really need to have the industry supportive and so I would urge us as an industry and working with out fellows in the public interest world and civil society to come up with a robust plan. That does not mean that legislation is not something that ultimately is at the end of that road but certainly right now the first step is discussion.

Mr. RUSH. All right. Please, yes sir?

Mr. SCOTT. Yes, I agree a baseline privacy law would be a reasonable next step.

Mr. RUSH. Yes, OK.

Mr. KNAPP. This is my first hearing. Is maybe an acceptable answer? I think as a cutting edge innovative company that really wants to offer a service that users love and they want for free I, you know, I think a high level privacy framework that sticks by tried and true principles would be beneficial. But I do have concerns when laws get too specific or focus on a snapshot in a moment of time as I think has been mentioned here today and may get outdated and problematic for some companies like us who are trying to innovate and offer services for free to comply. And so those would be my concerns about that approach.

Mr. RUSH. All right. Go ahead.

Mr. BENNETT. Mr. Rush, I think I could support a bill like that if the emphasis was on disclosure rather than on prohibitions of particular practices. And one feature that I would like to see in it is that once a consumer has opted into a data collection service, I think you should get a regular reminder or the opt-in shouldn't be perpetual. So when you opt-in to a service it works for a year then you have to get a notice and you have a choice of opting in again because I don't know how many Web sites I have given permission to, to collect information on me over the years that I have completely forgotten about.

Mr. RUSH. So your answer is yes?

Mr. BENNETT. I answered yes.

Mr. RUSH. OK. All right. Thank you. Mr. Rotenberg, since we need another vote from you. Why don't you answer again? I am just kidding. All right. The next question that I have is and please the same sequences for all the panel is do you believe that consumers should have the same sort of control if and how their information is selected? Do you believe that they should control if and how this information is used? Please answer a yes or no.

Ms. HARRIS. I think that the question of use is an important one and it seems to me that when you are authorizing a collection you ought to also be authorizing the purposes or you are authorizing that it can be used for multiple purposes. But I don't think, you know, simply saying you can have my data or not have my data answers the question. We use your data for marketing, opt-in, don't opt-in. We use your data for, you know, I mean I think there are some uses of data which are transactional that, you know, if you are ordering a product I think separately saying you can use my data to do what is necessary to process this transaction seems unnecessary but for uses that are not directly connected for the initial purpose of collection it is just a standard fair information practice then I think yes of course you have to authorize that.

Mr. RUSH. Sure. Next gentleman.

Mr. MCSLAW. I think in our case The Cable Act actually is a good example which says that when you give authorization for personally identifiable information, it doesn't take into account the use of that data for just rendering the business services. But once you go beyond that I think you do have to identify what the purpose is you would use it for.

Mr. ROTENBERG. Mr. Chairman, I would say yes and I would probably add in some other things too like ensuring security of the data that is collected and some access to the information and some accountability. I think the basic elements of a privacy bill and in fact The Cable Act is a good model or at least the pre-Patriot Act version was a good model from 1984. That is a good starting point.

Ms. ATTWOOD. Yes, we support transparency and control.

Mr. SCOTT. Absolutely and I think beyond that I agree that the consumer is not only entitled to know that their data is being used but three other things. One is intentionality, the other is behavior and the third is outcome. Why do you want my information? What are you going to do with it? And what does that mean to me as a consumer?

Mr. RUSH. Yes.

Mr. KNAPP. Yes we agree with the principles of transparency and control, as well.

Mr. RUSH. OK.

Mr. BENNETT. That is a yes for me, too.

Mr. RUSH. Thank you, Mr. Chairman. I appreciate you, sir.

Mr. BOUCHER. Thank you very much, Mr. Rush, and we look forward to coordinating closely with you as we develop the joint hearing between our two subcommittees and then thereafter as we develop privacy legislation which we will put forward in tandem.

Mr. RUSH. Nice of you to say, Mr. Chairman.

Mr. BOUCHER. And thank you for your presentation.

Mr. RUSH. You are a great Chairman.

Mr. BOUCHER. Thank you very much. The gentleman from New York, Mr. Weiner, is recognized for 5 minutes.

Mr. WEINER. Mr. Chairman, I won't take the full 5 minutes. It strikes me that some of the what gets hairy here is saying is defining what it is that you are checking the box to do. For example, is you say I want help in deciding what other products are out there that are being sold that I might be interested in. It is a pretty tough box to word. I mean it is a pretty tough disclosure to have any real meaning but I think by and large, consumers do like that. I mean I like it when you go to Amazon and it says we also have this for you. So I think one of the problems that we often face is that disclosure has tipping point that if you want it until the point that there is so much of it that it ceases to really disclose anything. And I think the part of the challenge that we have is trying to come up with terms of art that truly do encapsulate what we are trying to do. For example, you know, would you like to be told about other products you might be interested in. Theoretically, that can be just about anything. I mean it is concise and it is crisp and it probably is worded in a way that will entice people to check a box and I don't know how you have a second line that says but you are going to get a lot of stuff and a lot of companies that might be far removed from this shoe purchase might be getting information. And so I mean can you offer us any guidance on how to make this type of disclosure opt-in, opt-out truly useful to consumers without us all having to retain, you know, to go to lawyers.com to read what I am getting at Amazon.com. I don't know who would be best to tackle that? Whoever leans forward first.

Mr. ROTENBERG. Well, I mean, Congressman, it is an excellent point and it is one of the reasons I have suggested in my testimony not to place too much emphasis on opt-in or opt-out as the basis for privacy protection. Given a choice between opt-in and opt-out from the consumers' perspective, opt-in is preferable because it means more control but for many of the reasons you described, it won't be adequate for real privacy protection. For example, no one agrees to a security breach. In other words, you may check a box and give a company some information and some magnetic tape is going to fall off the back of the truck. You certainly didn't agree to that so there has to be a way I think within privacy law to get it to a broader range of issues for many of the reasons your described.

Ms. HARRIS. I agree with that. I think that the Congress has been stymied in moving that forward on privacy because of the sole focus being about opt-in and opt-out, and not looking more broadly at how to resolve some of these, you know, other questions. And we don't know how to give notice well in a way that consumers understand. You know, I think one thing to look to is we just passed landmark new privacy protections in the healthcare context and it could have gotten equally tied-up around opt-in and opt-out and it focused far more broadly, you know, about where sharing was appropriate and not appropriate, security protections. So while those, while there are places where consent is required, it is not just about that. And I think that we do get hung up sometime and we don't wind up with a framework so we need a framework. And we would start with fair information practices because that is transparency. That is collecting data only to the extent you need it for the transaction. It is giving people choices about other uses and it is making the explanation about those other uses.

Mr. WEINER. Right but before Ms. Attwood adds to this, even that is complicated, right?

Ms. HARRIS. Right, I am not saying this is easy.

Mr. WEINER. Right, I mean just about the transaction, well you bought the stereo. You should know about—do you mind if we share information with this speaker company and then you get information about that. I mean I agree it is that opt-in and opt-out is not the only way to do this and we are going to go far beyond that. But we have grown kind of culturally accustomed to the idea of having places that we kind of agree to what goes on. You know, when my credit card company says oh yes, well we told you about that. I am like, really that was page nine six months ago on the thing we told you about it. We are covered. So you are right, opt-in, opt-out is not everything but the way we have grown literate with how these things happen as citizens, there is some expectation that we are going to have some control over that.

Ms. HARRIS. Oh absolutely, I am not suggesting that we shouldn't.

Mr. WEINER. Right.

Ms. HARRIS. I am saying that even that is much harder and has not been done well online in most instances so, you know, passing this framework is the beginning but the assumption that we are going to get these practices right overnight, no, we are not.

Mr. WEINER. Go ahead, Ms. Attwood.

Ms. ATTWOOD. I just I guess I offer some hope in the context of if you approach this as a legal exercise then consent is something that is a, you know, it is a difficult proposition to get right. But if you approach this as actually what really is exploding online and the idea that in fact you are trying to get personalization and you are trying to get information that is all about me and you are trying to get a page that identifies my likes and dislikes, I have confidence that that in fact this industry using new and developing tools will be able to actually communicate more effectively to the customer and allow that kind of customization and that personalization to be an advance. If we think about this as a design feature, privacy is a design feature in what I am offering then it is in my interest as a commercial entity to make it very clear that proposition. That is why you see the success of Loopt. On one level, his service is extremely complicated. On the other level, the customer gets it right away, understands the value of proposition and that communication is something that as an industry I think I am optimistic that we can work to grow that communication and make it work for consumers.

Mr. WEINER. Thank you, Mr. Chairman.

Mr. BOUCHER. Thank you very much, Mr. Weiner. The gentlelady from the Virgin Islands, Ms. Christensen, is recognized for 5 minutes.

Ms. CHRISTENSEN. Thank you, Mr. Chairman, and this is a very interesting hearing for me. Privacy is an issue that is of very much concern to minority communities like the one I represent and it comes up whenever we talk about HIT and other issues related. Ms. Attwood, when you were asking about opt-in and opt-out and you talked about engagement it seemed as though you used that word deliberately and wanted to elaborate on it and I wanted to give you an opportunity to explain what you mean by engagement.

Ms. ATTWOOD. Sure, I actually think Mr. Rotenberg said it a lot better and but I think everybody on the panel has discussed it that when we talk about opt-in and opt-out, we really are limited in the concept of what we are trying to discuss when it comes to really ensuring that the customer is part of the decision about the use of the information and that is a broader concept. That is a concept that is engaging. That is a concept that is enticing. That is a concept of control. Opt-in, we have all been a part of opt-ins. I think the Congressman from New York described it where, you know, it is pages and pages and pages where the company is entirely protected and there is a checked box but it is not. The customer is not in fact really participating in that decision, you know, and so I am hopeful this industry can in fact rally around the idea of really bringing the customer into that decision and it can happen in a broader way.

Ms. CHRISTENSEN. I am kind of old fashioned and I am trying to remember when I see those kinds of boxes, I just want to skip them. Do people usually answer them and or do you have to opt-in or opt-out, just for my information, not as a swear. Do you have to answer it?

Ms. ATTWOOD. If it is designed that way, I mean they are designed differently but there are some that are forced screens or box where you can't get past it unless you do something so yes. There

are others that in fact don't require that but most times it is a service obligation to check that box.

Ms. CHRISTENSEN. And in the cases where you just ignore it and try to move on and you can, that is assumed to be an opt-out?

Ms. ATTWOOD. It would be possibly an opt-out. It really again depends on the design of that. It may be that you don't get the service.

Ms. CHRISTENSEN. Did you want to say something, Ms. Harris?

Ms. HARRIS. Yes, I do want to agree with Ms. Attwood on the question of can industry doing this. I mean in discussing this with Mr. Weiner, it is very hard but when industry chooses to do this, when they choose to do it sort of at the beginning and do privacy by design rather than privacy by law, it can be accomplished. Loopt is an example. There are several examples in the online healthcare space where from the very beginning this has been built in, in a way that consumers can use. So I, you know, it is hard to say that we are in this environment of such technological innovation and we can't figure out how to use that technological innovation to make this simpler. I think we can. I think frankly a privacy framework will encourage that but I do think at the end of the day it is going to have to be, you know, a combination. The law by itself in the absence of companies stepping up and doing that and that is what is going to have to happen.

Ms. CHRISTENSEN. OK. I thought Mr. Bennett's suggestion of having to go back periodically and opt-in was a good one. Does that happen now and if doesn't, would you all support periodically having to go back and review that question?

Mr. ROTENBERG. We have actually recommended that the right way to understand consent is that you should be able to opt-in when you choose to have your data used in a way and then opt-out at the point that you want to discontinue the use and I think Mr. Bennett's comment captures that but any time you choose to leave a service—this came up recently with Facebook, for example.

Ms. CHRISTENSEN. Yes.

Mr. ROTENBERG. Facebook wanted to tell users well you leave the service. We will keep your data and the user said well that is not right. I mean if we leave the service we want you to delete the data.

Ms. CHRISTENSEN. Right.

Mr. ROTENBERG. And Facebook agreed and I think that is people's intuition and it is really fair, and when companies go against it then there is a problem.

Ms. CHRISTENSEN. Right.

Ms. HARRIS. I think it is going to be a very important concept for the ISPs if they are to move into this space because for some people who are not also using an ISP's e-mail service, they may not be communicating with their ISP except at, you know, initially to sign up or get a bill so the potential to think about screens that come on, you know, that explain what you agreed to and give you a choice to change your mind, I think it is going to be a critical part of it.

Mr. SCOTT. It strikes me that whether we are talking about reminders which I think is a great idea or engagement or clarity and transparency, we are really talking about our different forms of

consumer education because the real problem is that most consumers don't have any idea what the 10,000 words of six point font means when they check the box at the bottom and oftentimes, sometimes those boxes are pre-checked or you can't buy the shoes unless you check the box and so in many ways I think we need to be thinking about ways to help consumers understand exactly what it is that they are signing up for and what that means and what comes to my mind is the little glossy one-pager that my power company sends me every winter to try to advise me on how to save money on my power bills. It has got pictures. It is in big letters. I read it. I have actually found some helpful tips there. That is sort of is what I think of as engagement when I hear you say that and I think that is the kind of consumer education that can help us fix this problem.

Ms. CHRISTENSEN. Thank you. Thank you, Mr. Chairman.

Mr. BOUCHER. Well, thank you very much, Ms. Christensen. I want to say thank you to all of the witnesses for their extremely informative testimony today. This has been an engaged conversation and as we close this hearing, I simply want to note that I personally concur completely with the suggestions that many have made here over the course of the last hour that what is needed is not just a decision between opt-in and opt-out but also a framework for privacy protection. And I hasten to note that the legislation that Mr. Stearns and I put forward some several years ago which will be the starting point and the foundation for our privacy bill this year, contains exactly the kinds of formulas that many on the panel have suggested and that is that any service that collects information about a customer must disclose what information that is collected and how that information is used and then provide the appropriate opportunity for that customer to act on the information, whether that be by opt-in or opt-out. So opt-in taken by itself, is meaningless. There has to be an adequate description of what conduct the particular user is authorizing for it to have content and meaning and offer real protection. We get that and that will be very clearly a part of the foundation of the measure that we move forward with later.

So with that having been said and acknowledged, let me thank this panel for its contributions to our understanding of the network technologies that have privacy implications for users and suggest that we probably are going to be consulting with you at greater length as we move forward to have our joint hearing with the other subcommittee and also to draft this legislation. You have been very helpful to us. We appreciate your participation and with that said, this subcommittee stands adjourned.

[Whereupon, at 12:10 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

Testimony of Scott Cleland, President, Precursor LLC
“The Blind Eye to Privacy Law Arbitrage by Google – Broadly Threatens Respect for Privacy”
Before the House Energy & Commerce Subcommittee on Internet Hearing, July 17, 2008

I am Scott Cleland, President of Precursor LLC, an industry research and consulting firm. I am also Chairman of NetCompetition.org, a pro-competition e-forum funded by telecom, cable and wireless broadband companies. My testimony today reflects my own personal views and not the views of any of my clients.

The current patchwork of U.S. privacy laws, the lack of a holistic approach to Internet privacy, and selective oversight of privacy problems – have combined to create perverse incentives for some companies to: arbitrage privacy laws and push the privacy envelope. As a result, invasion/abuse of privacy is among the most serious problems users face on the Internet. **The lack of a holistic, comprehensive and balanced approach to privacy law and oversight is a serious threat to American’s privacy.**

Broadband companies. (telecom, wireless and cable) have long been subject to strict privacy laws (sections 222, 551 & the ECPA), which created serious consequences for the misuse of personally identifiable information without a user’s permission. Consequently, broadband companies have developed extensive policies, procedures and practices to respect users’ privacy and protect personally identifiable information. This Subcommittee’s oversight of experimentation by some, with “deep packet inspection” for advertising purposes, is entirely appropriate. Existing laws appear to cover these practices so oversight by Congress is expected.

I am concerned however, that selective oversight of only broadband privacy matters fosters a blind eye to arbitrage of privacy laws by application companies like Google, Yahoo and others. This creates perverse incentives for companies not covered by U.S. privacy laws to push the envelope on privacy to gain competitive advantage. **Americans’ privacy should not be an unrestricted commodity to sell to the highest bidder or to gain competitive advantage.**

Specifically, I am troubled with the selective broadband focus of this hearing, because privacy is a cross-cutting, big picture issue that knows no boundaries between the access, application and content “layers” of the Internet. To add balance and to focus on the most serious threat to Americans’ privacy, I humbly suggest the Subcommittee hold another hearing entitled: *“Why Google Knows Everything About You: Unauthorized Web Surveillance and Privacy Law Arbitrage.”*

By turning a blind eye to what Google, the worst privacy offender on the Internet, is doing to systematically invade and abuse Americans’ expectation of privacy, Congress is perversely encouraging copycat behavior by “deep packet inspection” advertising entrepreneurs who see that there is a huge privacy double standard to arbitrage. Companies like NebuAd are essentially just following the privacy-arbitrage leader – Google.

To illustrate my point of the extreme privacy law arbitrage that is occurring in the U.S. marketplace today, I explain in detail in my written testimony how Google is the single worst arbitrageur of privacy laws and the single biggest threat to Americans’ privacy today.

Case Study: How Google Systematically Threatens Americans’ Privacy:

1. Google’s radical “publicacy” mission is antithetical to privacy.
2. Privacy is not a priority in Google’s culture.
3. Google gives privacy “lip service.”
4. Google threatens the privacy of more people than most any other entity.
5. Google collects/stores the most potential “blackmail-able” information.
6. Google’s track record does not inspire trust.

As others have said, information is power. Power corrupts. Absolute power corrupts absolutely. Google’s market power over private information is corrupting Google, just like former FBI Director J. Edgar Hoover was corrupted by his power and mastery of personally-sensitive information. Google’s unprecedented arbitrage of privacy law combined with its exceptional lack of accountability is fast-creating this era’s privacy-invading, unaccountable equivalent: “J. Edgar Google.” Remember the timeless insight, those who don’t learn from history -- are doomed to repeat it.

126

**Written Testimony of
Scott Cleland
President, Precursor LLC**

**“The Blind Eye to Privacy Law Arbitrage by Google
-- Broadly Threatens Respect for Privacy”**

**Before the
House Energy & Commerce Subcommittee
On Telecommunications and the Internet**

**Hearing on:
“What Your Broadband Provider Knows About Your Web Use:
Deep Packet Inspection and Communications Laws and Policies”**

July 17, 2008

I. Introduction

Mr. Chairman and Members of the Subcommittee thank you for the honor of testifying on the important subject of Internet privacy. I am Scott Cleland, President of Precursor LLC, an industry research and consulting firm, specializing in anticipating the future of the converging techcom industry. I am also Chairman of NetCompetition.org, a pro-competition e-forum funded by telecom, cable and wireless broadband companies. My testimony today reflects my own personal views and not the views of any of my clients.

II. The Problem of Privacy Law Arbitrage and Selective Privacy Oversight:

The current patchwork of U.S. privacy laws, the lack of a holistic approach to Internet privacy, and selective oversight of privacy problems – have combined to create perverse incentives for some companies to:

- Arbitrage privacy laws,
- Try and “fall between the cracks” of privacy oversight, and
- Push the privacy envelope.

As a result, invasion/abuse of privacy is among the most serious problems users face on the Internet. The lack of a holistic, comprehensive and balanced approach to privacy law and oversight is a serious threat to American’s privacy.

Broadband companies, (telecom, wireless and cable) have long been subject to strict privacy laws (sections 222, 551 & the ECPA), which created serious consequences for the misuse of personally identifiable information without a user’s permission. Consequently, broadband companies have developed extensive policies, procedures and practices to respect users’ privacy and protect personally identifiable information. Like medical providers operate under HIPPA privacy protections and financial services providers operate under FCRA/FDCPA privacy protections, broadband providers operate under sections 222, 551 and the ECPA, privacy protections. As a result, the broadband, medical and financial industries have **made respect for privacy an integral part of their business models and cultures.**

This Subcommittee's oversight of experimentation by some, with "deep packet inspection" for advertising purposes, is entirely appropriate. Existing laws appear to cover these practices so oversight by Congress and regulators is appropriate and expected.

I am concerned however, that selective oversight of only broadband privacy matters fosters a blind eye to arbitrage of privacy laws by application companies like Google, Yahoo and others. This creates perverse incentives for companies not covered by U.S. privacy laws to push the envelope on privacy to gain competitive advantage. **Americans' privacy should not be an unrestricted commodity to sell to the highest bidder or to gain competitive advantage.**

- Specifically, I am troubled with the selective broadband focus of this hearing, because privacy is a cross-cutting, big picture issue that knows no boundaries between the access, application and content "layers" of the Internet.
 - If the Subcommittee holds a hearing entitled: *"What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies"* – to add balance and to focus on the most serious threat to Americans' privacy, I humbly suggest the Subcommittee hold another hearing entitled: *"Why Google Knows Everything About You: Unauthorized Web Surveillance and Privacy Law Arbitrage."*
- By turning a blind eye to what Google, the worst privacy offender on the Internet, is doing to systematically invade and abuse Americans' expectation of privacy, Congress is perversely encouraging copycat behavior by "deep packet inspection" advertising entrepreneurs who see that there is a huge privacy double standard to arbitrage.
 - If you are a broadband provider strict privacy laws apply, if you are an "application" provider like Google, it's the Wild West – there's no privacy protection.
 - Like water seeking its own level, market forces can be expected to arbitrage the huge gaps in privacy protection among companies.
 - Companies like NebuAd are essentially just following in the footsteps of the privacy-arbitrage leader – Google.

To illustrate my point of the extreme privacy law arbitrage that is occurring in the U.S. marketplace today, let me explain in detail how Google is the single worst arbitrageur of privacy laws and the single biggest threat to Americans' privacy today.

III. Case Study: How Google Systematically Threatens Americans' Privacy:

To begin, I am not alone in believing Google's privacy practices are a particularly serious consumer protection problem.

- **Privacy watchdog, Privacy International, ranked Google worst in its world survey on privacy in 2007 and described Google as "hostile to privacy."**
- EPIC, CDD, and USPIRG filed suit with the FTC last year challenging Google's privacy practices as deceptive trade practices.
- Recently, a broad coalition of privacy advocates pressured Google to finally comply with California privacy law and put a link to their privacy policy on their home page.

1. Google's mission is antithetical to privacy.

- Google's megalomaniacal "*mission is to organize the world's information and make it accessible and useful.*"
 - **Google's mission is so uniquely antithetical to privacy – it actually warrants the creation of a new term: "publicacy."**
 - Google's unique and radical "publicacy" mission believes "the world's information," is, and should be public not private. (Note the mission statement puts no qualifier on "information" other than "the world's.")
- The fact that most of the world's most valuable information is *copyrighted or owned by others* hasn't stopped Google from making other's property universally available – without permission or compensation. As a result, several different content industries are suing Google for theft. Google supports radical copyright reform to remake the Internet

into a less-proprietary, “information commons” where most all content is free to the user and supported by Internet advertising -- the business that Google dominates.

- The fact that much of the world’s information is also *private*, or enables privacy because it is not easily accessible publicly by anyone, hasn’t stopped Google from trying to make this *private* information *publicly* accessible. The business reason for this is that Google knows that the most valuable information is private (scarce) information that was not available before. Google also knows that its competitive advantage is its world-leading “database of user intentions,” i.e. search histories on several hundred million Google users worldwide. Google also understands that it can earn a premium because it knows more private information on users’ intentions, preferences and secrets than any other company in the world – by far. Simply, Google’s business edge is that it collects, stores and uses more private information than any other entity in existence, which enables it to “target” “relevant” advertising better than anyone else.
- The fact that Google’s web “crawlers” are the world’s most pervasive and invasive, Google indiscriminately searches websites for whatever it can find, and automatically assumes if their crawlers can find it, it must be “public” information. This indiscriminate web crawling has resulted in Google exposing private information like social security numbers, as Google did in making hundreds of California university students’ social security numbers public -- as reported by the Sacramento Bee (3-7-07.)

2. Privacy is not a priority in Google’s culture.

- Google celebrates an “innovation without permission” culture. Google’s obsession with innovation comes at a cost, because it comes with a cultural disdain for internal controls, management supervision, and internal vetting of issues for privacy concerns. Let me illustrate this cultural disdain for privacy with three high-profile examples of Google proceeding full-speed-ahead with “beta” releases -- without regard to privacy implications of their actions.
 - Google introduced gmail, which enables Google to automatically read the content of users’ private gmail messages in order to send them “relevant” advertising –

without meaningful internal privacy review. This caused a widely reported public uproar over users' privacy being abused.

- Google introduced Google Earth, which exposed the roof tops of the White House, public buildings and military installations, without meaningful internal review of the privacy, safety, or national security implications. The uproar that ensued over this suggests Google learned little from the gmail incident about the importance of internal review to address external concerns like privacy.
- Google then introduced StreetView, which is video of people's homes, apartments and neighborhoods, without meaningful internal review of the privacy or safety concerns involved. The uproar over this invasion of privacy is so significant that Google is very secretive about where and when Google's "spycars" will be videoing a particular neighborhood in order to protect the safety of the Google drivers from irate residents.
- The inescapable conclusion from this pattern of behavior is that Google's culture exhibits a fundamental and sustained disdain for privacy.

3. Google gives privacy "lip service."

- Only this month did Google begrudgingly comply with longstanding California Privacy law to post a link to their privacy policy on their webpage. Google's founders did not want to "clutter" the signature simplicity of their homepage with the addition of another word. Google's leaders spoke loudly on their assessment of the value of privacy policies with their stubborn recalcitrance on this most basic of privacy compliance. The message internally is that privacy is not a priority to the founders. We also know that organizations listen and follow the cues from their leaders about which values to follow in conducting business.
- Google has not bothered to update its privacy policy since October 14th, 2005 despite a number of major external developments that objective observers would think would merit an update or a change in their privacy policy.
 - Since the last update, Google has entered several new businesses which operate under very different privacy laws:

- YouTube – viewing habits;
 - Feedburner – reading habits;
 - GrandCentral – voiceprints and wiretapping;
 - DoubleClick – ad viewing
 - (Note: a few years ago the FTC sanctioned DoubleClick for its privacy practices.);
 - Google Health (which arbitrages HIPPA); and
 - FriendConnect (after state Attorney Generals acted on privacy/safety related issues of minors.)
- In the fall of 2007, Privacy International ranked Google worst in its world survey, and called the company “hostile to privacy.”
 - In 2007, privacy watchdog EPIC, sued Google via the FTC review of the Google-DoubleClick merger, for deceptive trade practices.
 - In late 2007, the FTC staff proposed new behavioral advertising privacy principles that run counter to Google’s current privacy practices.
- If Google really cared about privacy and it was an important priority, wouldn’t Google have updated its privacy policy to adapt to any of the above mentioned developments? Not only does Google not lead by example on privacy matters, it doesn’t even follow others lead.

4. Google threatens the privacy of more people than most any other entity.

- Google-DoubleClick track the search histories and ad-viewing habits of an estimated 90% of global Internet users, approaching a billion people worldwide.
- Google has the largest network of advertisers, ~1,000,000 compared to Yahoo’s ~300,000 and Microsoft’s ~75,000.
- Google has relationships with over 1 million websites, orders of magnitude more content relationships than its competitors.
- What this means is that **Google has both the means and the business model to learn more private information about more people than any other company in the world.**

5. Google collects/stores the most potential “blackmail-able” information.

- Consider the depth and breadth of intimate information Google collects:
 - *What you search for;*
 - (a Ponemon Institute survey of 1,000 Google users found that 89% thought that their searches were private and 77% thought Google searches could not reveal their personal identities – wrong on both accounts.)
 - *Where you go on the web;*
 - Google has pervasive unauthorized-web-surveillance capability (web tracking/stalking) through a combination of Google’s search, Google’s cookies, DoubleClick’s ad-view recording capability, Google’s extensive content affiliate network of hundreds of thousands of sites, and the wide variety of Google apps.
 - *What you watch -- through YouTube;*
 - (Remember Supreme Court nominee Robert Bork was politically attacked for the videos he rented.)
 - *What you read -- through Google News, Feedburner and Blogger.*
 - *What you say -- in your emails through gmail’s automated reader.*
 - *What you produce -- in Google Docs or spreadsheets.*
 - (In return for the free Google Apps like Docs and spreadsheets, users grant Google some search rights in perpetuity to any content a user produces using Google’s Apps.)
 - *What your family and friends look like -- through Picassa images.*
 - *Your medical conditions, medications, and medical history -- through Google Health.*
 - *Your purchase habits -- through Google Checkout.*
 - *Your call habits and voiceprint -- through Google Talk.*
 - *Your travel habits and interests -- via Google Maps.*
 - *Your interest in other people/places -- via Google Earth & StreetView.*
 - *Your personal information -- through Orkut (social networking) Gmail, Google Checkout, etc.*

- *Where you go/hang out* -- through Google wireless ventures and Android.
 - *Where you'll be or where you were* -- through Google Calendar.
 - The scale and scope of Google's unauthorized-web-surveillance is truly Orwellian "Big Brother." While Google is not the Government, all this private information that Google collects and stores is certainly available to the Government via subpoena.
 - It is also important that this capability of Google's is very different from Microsoft reach because as a software provider, your private information mostly resides on your PC where you control it.
 - In stark contrast, all of the private information listed above that Google collects *resides on Google's servers.*
- 6. Google's track record does not inspire trust.**
- Google does not fairly represent its business to users.
 - Google's rhetoric and public relations intimate that Google works for users – they don't. Google is not paid by users – Google is paid by advertisers and websites.
 - Like investment banks hurt investors during the bubble for not disclosing that their research had a financial conflict of interest, Google puts users at serious risk by not disclosing to them that Google has a financial conflict of interest in looking out for advertiser/website/Google interest before the users' interest.
 - How this conflict could hurt consumers today is that when websites are infected with dangerous malware like phishing for ID theft, Google has not been flagging certain search results as dangerous, when doing so would protect users from sites Google knows not be safe. They are being silent and not protecting users from potential harm because that would discourage traffic, clicks and revenue from Google's real clients: advertisers and websites.
 - If the Ponemon survey of Google's users is even remotely accurate, most consumers do not understand that they have forfeited their privacy to Google in return for Google's

free applications. In other words, few people understand that Google thinks they have users' full permission/assent to sell their privacy to the highest bidder.

- Another trust undermining aspect of Google's business is the rampancy of fraud in Google's model.
 - Most people are not aware that click-search is one of the most fraud-prone industries in America. Click Forensics, which is the leading industry tracker of web fraud, estimates that 28% of all Internet clicks are fraudulent.
 - The dirty little secret here is that the gross-revenue business model for search, which was pioneered by Google, makes money off of fraudulent clicks. In other words, Google's gross revenue model does not have a financial incentive to be honest.
 - It is hard to imagine another legal industry in America that would tolerate a 28% gross fraud rate!
- Google also does not inspire trust because **Google's words don't match its deeds**. It is the master of the slippery, self-serving, double-standard:
 - Google's mission is to organize the world's information to make it accessible, when Google is among the most secretive, non-transparent, 'black box' public entities anywhere.
 - Google pushes "open" everything for everyone else, open access, open source, open social, open handset, open spectrum, but the auction process that is at the core of Google's business model is not open but an opaque 'black box' that users cannot see into.
 - Google supports net neutrality regulation for its broadband competitors, but maintains that Google, the world's most dominant access point for the Internet, should not be subject to net neutrality regulation.
 - Google aggressively protects its intellectual property of copyrights and patents, while strongly supporting "information commons" reforms that would decimate the intellectual property rights of their competitors.
 - Google runs its not-for-profit Google.org as a for-profit division of Google, when every other corporation in America abides by the clear separation of for-profit and not-for-profit entities to avoid even the appearance of tax evasion or impropriety.

IV. Conclusion:

The lack of a holistic approach to Internet privacy combined with selective oversight of privacy problems encourages some companies to try and “fall between the cracks” of privacy law, to arbitrage privacy laws and to push the privacy envelope. This is unfortunate because invasion/abuse of privacy is among the most serious problems users face on the Internet. **In short, the lack of a holistic, comprehensive and balanced approach to privacy is a serious threat to American’s privacy.**

Vigilant oversight of broadband companies subject to privacy law is appropriate. What is not appropriate is discrimination against broadband providers as the only companies that warrant privacy oversight. The greatest risk comes from application providers like Google and Yahoo, which are not subject to privacy law, and are arbitraging that legal gap, as a competitive advantage to the serious detriment of Americans’ privacy. Given Google’s exceptional and increasing market power over the business of the Internet, it appears as if **the Subcommittee risks turning a blind eye to the single biggest unaddressed threat to Americans’ privacy.**

As others have said, information is power. Power corrupts. Absolute power corrupts absolutely. Google’s market power over private information is corrupting Google, just like former FBI Director J. Edgar Hoover was corrupted by his power and mastery of personally-sensitive information. Google’s unprecedented arbitrage of privacy law combined with its exceptional lack of accountability is fast-creating this era’s privacy-invading, unaccountable equivalent: “J. Edgar Google.” Remember the timeless insight, those who don’t learn from history -- are doomed to repeat it.

Attachment I:

Precursor Blog posts on Google & Privacy:

J. Edgar Google: Information Is Power + No Accountability

- <http://www.precursorblog.com/content/j-edgar-google-information-is-power-no-accountability>

Can you trust Google to obey the rules? Is Google accountable to anyone?

- <http://www.precursorblog.com/node/769>

Why Google storing personal health records is a really bad joke -- the public should be worried...

- <http://www.precursorblog.com/node/762>

Google's Privacy Lip Service

- <http://www.precursorblog.com/content/googles-privacy-lip-service>

Google protecting its privacy to invade your privacy; Why Google is the King of Double Standards:

- <http://www.precursorblog.com/content/google-protecting-its-privacy-invade-your-privacy-why-google-king-double-standards>

J. Edgar Google compiling personal YouTube viewing dossiers

- <http://www.precursorblog.com/content/j-edgar-google-compiling-personal-youtube-viewing-dossiers>

Response from Leslie Harris, President/CEO Center for Democracy & Technology to Questions from Rep. Stupak from April 23d, 2009 Hearing "Communications Networks and Consumer Privacy: Recent Developments."

1. In your testimony you contend that "consent has its limitations." Do you believe that establishing a strict "opt in" regime is not enough to addressing privacy concerns with using DPI for behavioral advertising?

As noted in my testimony, the Fair Information Practices (FIPs) have long been recognized as the comprehensive set of principles required for protecting personal data in a wide array of contexts. While consent plays an extremely important role within the FIPs, on its own it is often not enough to ensure full privacy protection. When consent is instead complemented by robust notice, meaningful choices, limitations on data use and retention, consumer access to collected data, appropriate redress procedures, and robust security safeguards, the risks to consumer privacy are significantly reduced.

In the particular case of DPI used for behavioral advertising, while we believe that opt-in consent is necessary, it is not sufficient by itself to ensure complete privacy protection. Consider, for example, a DPI-based behavioral advertising system in which all Internet communications of all subscribers were retained indefinitely in personally identifiable form, but with no means for subscribers to view the data held about them. Even if subscribers consented to the collection of their data, the storage of such massive amounts of highly sensitive communications would create huge, unnecessary risks for those subscribers, including the risk that the data would be lost, stolen, or become fodder for legal requests. Because each of the FIPs is an integral component to protecting privacy, opt-in consent cannot serve on its own as a silver bullet.

2. What is your position on having affirmative consent or a mandatory opt-in from consumers tied with providing that consumer information on what is happening with their data, how it is collected, and who is receiving it before using their personally identifiable information for the purpose other than providing them service?

[I think this question is about consent for secondary uses. Not sure how explicit we want to be – my response below is accurate but vague.-ALC]

We firmly believe that prior to having their data collected, consumers should be provided with information about who is collecting their data, the purpose of the collection, and how the data will be shared. If a service provider later decides to use or share the data for a different purpose, consumers should have the opportunity to consent to the new data use or disclosure.



National Cable & Telecommunications Association
25 Massachusetts Avenue, NW – Suite 100
Washington, DC 20001
(202) 222-2300
www.ncta.com

Kyle McSillarow
President and CEO

(202) 222-2500
(202) 222-2514 Fax

May 27, 2009

The Honorable Bart Stupak
2268 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Stupak,

Thank you for your questions dated May 13, 2009, stemming from a hearing at which I testified entitled "Communications Networks and Consumer Privacy: Recent Developments." The Subcommittee on Communications, Technology and the Internet held this Hearing on April 23, 2009.

Below you will find answers to each question you submitted to me. Please do not hesitate to contact me if there are any other issues that need to be addressed.

Sincerely,

A handwritten signature in black ink, appearing to read 'K. McSillarow', followed by a horizontal line.

Kyle McSillarow
President & CEO

Q1. In your testimony you outlined the obligations the Cable Act of 1984 has required of your member companies. Do you believe that, pending legislation from this Committee on privacy should attempt to harmonize those privacy protections across all Internet providers, wireline and wireless?

As I stated in my testimony, NCTA believes that achieving and sustaining subscribers' trust requires adherence to privacy framework for online behavioral advertising that addresses four principles: first, giving customers *control*; second, providing *transparency* and *notice*; third, *safeguarding personal information*; and fourth, providing customers with *value*. We think all industry wireline and wireless stakeholders should participate in the development of this framework, in the form of self-regulatory principles.

Q2. In your testimony you state that cable operators must obtain prior customer consent before collecting personally identifiable information. What are the guidelines for cable companies in acquiring affirmative consent? Is there an established practice on how that consent is acquired? When is that consent obtained normally? (fine print, obtain subscribing to service, via email?)

Cable operators are required by section 631(b)(1) of the Cable act to obtain the "prior written or electronic consent" of a subscriber in order to use the cable system to collect personally identifiable information concerning the subscriber, unless necessary to render services or to detect unauthorized reception. There are no industry guidelines for acquiring affirmative consent, but each of our member companies obtains prior written or electronic consent where required to do so. Written consent may include a signature on the work order at the time of installation. An example of electronic consent is using a remote control to select an on-screen option to order a product or obtain more information about a product being advertised. As I stated in my testimony, none of our cable Internet Service Providers ("ISPs") currently uses network-based technologies to collect PII for the purpose of delivering behavioral advertising.

Q3. What is your position on having affirmative consent or a mandatory opt-in from consumers tied with providing that consumer information on what is happening with their data, how it is collected, and who is receiving it before using their personally identifiable information for the purposes other than providing them service?

We believe an affirmative consent requirement should include the provision of the information described in your question. In this regard, section 631(a) of the Cable Act requires cable operators to give separate, written notice (at the time of the initial service agreement and annually thereafter) clearly and conspicuously informing subscribers of the nature of the PII collected; how it will be used; the frequency, nature, and purpose of any disclosure (including identification of the types of third party recipients); the period for which PII will be kept; and the subscribers' rights to enforce statutory limitations with respect to the collection and disclosure of information. This annual notice provides subscribers with the information described in your question prior to any collection or disclosure that requires a subscriber's prior written or electronic consent.

ELECTRONIC PRIVACY INFORMATION CENTER

epic.org

May 27, 2009

Chairman Henry Waxman
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Waxman,

This letter responds to your letter of May 13, 2009 letter regarding the April 23, 2009 hearing "Communications Networks and Consumer Privacy: Recent Developments."

Congressman Stupak asked:

What is your position on having affirmative consent or a mandatory opt-in from consumers tied with providing that consumer information on what is happening with their data, how it is collected, and who is receiving it before using their personally identifiable information for the purposes other than providing them service?"

In terms of obtaining consumer consent, this approach would establish a high standard and would be preferable to other types of consent that have been proposed. At the same time, there are at least four problems with seeking consumer consent for what is essentially permission to intercept private communications for marketing purposes. First, the consent would really have to be limited to those specific activities that the company has proposed at the time consent has been obtained. Consent would not be meaningful if, for example, it was provided for the purpose of "providing a better user experience." Second, consent to use personally identifiable information obtained from a private communication would almost certainly invite new and unanticipated uses. Personal information, including medical information, might be revealed in the course of a personal communication. Consent to disclosure to third parties could be problematic if not fully considered. Third, privacy obligations, even when consent is obtained, are ongoing. No one would consent to the improper release of their personal data by means of a security breach. Companies would still have a responsibility to safeguard the information they obtained. This is the reason that the objection of the European Commission to the UK proposal to allow behavioral targeting from private communications was based on (1) the failure to obtain adequate consent, and (2) the failure to ensure ongoing privacy

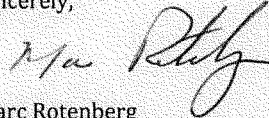
1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 483 1140 [tel]
+1 202 483 1248 [fax]
www.epic.org

protection for the data obtained. Fourth, a communication between two entities, such as a phone call, an email, even an HTTP connection between a client and a server, is essentially a private communication. There is something a little counterintuitive, and certainly contrary to the expectation of privacy, to enabling third party access to private communications. In the past, this has typically occurred only to ensure provision of the service, e.g. to maintain line quality, or to comply with a legal requirement, such as a warrant or subpoena.

Notice and consent has never been a particularly effective technique for privacy protection. But it seems a particularly weak approach when the information concerned is the content of a private communication used for marketing purposes. That is the reason I recommended that the Committee not encourage consent techniques in this context.

Thank you for the opportunity to participate in the hearing and to provide additional information for the Committee.

Sincerely,

A handwritten signature in dark ink, appearing to read "Marc Rotenberg", written in a cursive style.

Marc Rotenberg
EPIC Executive Director



Dorothy Attwood T: 210-351-2725
 Senior Vice President – Public Policy and Chief Privacy Officer F: 210-886-1025
 AT&T Services, Inc.
 530 McCullough – Suite 11-J-20
 San Antonio, TX 78215

May 13, 2009

The Honorable Anna Eshoo
 U.S. House of Representatives
 205 Cannon House Office Bldg.
 Washington, DC 20515

Dear Congresswoman Eshoo:

I am writing in response to your letter to Randall Stephenson, dated April 24, 2009, regarding AT&T's recent testimony before the House Subcommittee on Communications, Technology and the Internet. We are glad to address your apparent misapprehension regarding AT&T's current online behavioral advertising business plans and vendor relationships.

Online advertising is a complex ecosystem, and the subset identified as "behavioral advertising" encompasses a wide scope of activities.¹ For this reason, AT&T has endeavored clearly to explain its practices and perspectives with regard to behavioral advertising when engaged directly with members of Congress, regulators and other stakeholders. Among other things, we corresponded with leadership of the House Energy and Commerce Committee in August of last year,² and were asked to testify before both the Senate Commerce Committee and, most recently, the House subcommittee of which you are a member. Because AT&T operates in many capacities in the online ecosystem – that of Internet service provider ("ISP"), website publisher, and online advertiser of our products and services – we have been careful to address all inquiries with specificity and with reference to the particular AT&T role implicated.

In particular, in response to recent congressional interest concerning the plans of network-based service providers, such as AT&T, to launch new behavioral advertising lines of business, we have explained that:

AT&T does not engage in the behavioral advertising that is the focus of your inquiry, specifically the tracking of a consumer's overall web search and web browsing activities – by tracking either the person or particular computer – to create a distinct profile of the consumer's online behavior (Overall Behavioral Targeted Advertising).³

AT&T has articulated at every turn what it does and does not do in the context of any behavioral advertising model that has been the subject of congressional interest. We do not, through the use of deep packet inspection or any other technology, track our customers' overall web browsing

¹ See, e.g., FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising, February 2009 ("FTC Staff Report"), pp. 2-4.

² Letter from Dorothy Attwood, Senior Vice President, Public Policy, and Chief Privacy Officer, to Representatives Dingell, Barton, Markey and Stearns, dated August 13, 2008 ("August letter").

³ August letter, pp. 1-2 (emphasis added, footnotes omitted).

Representative Anna Eshoo
 May 13, 2009
 Page 2

activity across unrelated websites to create a profile of a particular consumer's interests or activity. Further, we do not collect or provide information about our customers' overall web browsing or search activity to any vendor, including for the purpose of delivering online behavioral advertising. This was the case when we wrote to Congress in our August letter, it was the case when we testified before both congressional committees, and it is the case today.

Moreover, even though the focus of public and congressional interest has centered on AT&T's potential plans for employing network-based technologies to enter the behavioral advertising business, for the sake of completeness and clarity, we have also referenced AT&T's activities as a website publisher and advertiser of our own products and services.⁴ In these contexts, AT&T is but one of literally thousands of others businesses that manage websites or market their own products and services online. As is commonly the case for entities with a retail Internet presence, we observe usage on our own commercial Internet sites to optimize the user experience and advertise our own products. On some of our web properties, we make space available to other advertisers through advertising networks. And, we work with online marketing firms to ensure that our own advertising – which promotes the AT&T brand and our various products and services – is delivered as effectively as possible.

It is in our role as a typical advertiser of our own products and services that AT&T has had a business relationship with Audience Science since approximately 2005. Audience Science is one of a number of online marketing firms that assist AT&T in reaching potential customers and placing AT&T's advertisements on other websites. Audience Science does not use deep packet inspection technology, but does use cookie-based methods to develop a view on the types of advertisements that consumers might find most relevant or useful, and to assist advertisers and website publishers, such as AT&T, to deliver ads for products and services based on that view. Audience Science discloses its practices and its privacy policies on its website, and, most pertinently, provides a button on its home page that allows consumers to opt out of its tracking capabilities.⁵ In addition, Audience Science is a member of the National Advertising Initiative ("NAI"), which, among other things, provides consumers with the ability to opt out of any NAI member's behavioral advertising program.⁶

Notably, AT&T's online practices as a website publisher or advertiser have never been a focal point of our exchanges or testimony, presumably because there is little to be learned from AT&T – as compared to thousands of other companies with an online presence – about these practices. Indeed, to the extent you have questions concerning the consumer-tracking and behavioral advertising capabilities of Internet website publishers, advertising networks and search engines, the commercial leaders in this space, such as Google and Yahoo!, undoubtedly could explain in greater detail the nature and terms of their existing overall web practices and privacy policies.

⁴ See, August letter, p. 3; Statement of Dorothy Attwood before the Senate Committee on Commerce, Science and Transportation, dated September 25, 2008, p. 6 fn. 3.

⁵ See, <http://www.audiencescience.com/>

⁶ See, http://www.networkadvertising.org/managing/opt_out.asp

Representative Anna Eshoo
May 13, 2009
Page 3

Finally, regarding your last question, AT&T has not just called on its advertising partners to improve transparency and control for consumers. Rather, we have called on the entire online advertising ecosystem – including advertising networks, search engines, ISPs, advertisers and publishers – to adopt a unified, consumer-centric policy framework built on a foundation of transparency, consumer control, privacy protection, and consumer value. And, we have more broadly urged those entities and stakeholders that, unlike AT&T, are today employing behavioral advertising capabilities that invisibly track users' overall web activity to develop a holistic and technology neutral privacy framework. This is necessary precisely because the complex relationships among behavioral advertising networks, advertisers and website publishers make effective customer transparency and control possible only through an industry-wide effort. We are more than willing to work with all entities in the ecosystem to create standards that can advance consumer interests.

We trust that the foregoing addresses your questions. We would, of course, be glad to provide you a further briefing on any aspect of AT&T's privacy policies. In the meantime, please let us know if you require additional information.

Respectfully submitted,



Dorothy Attwood
Senior Vice President – Public Policy
and Chief Privacy Officer



Timothy P. McKone
*Executive Vice President
Federal Relations*

AT&T Services, Inc.
1133 21st Street, NW
Suite 900
Washington, DC 20036

T: 202.463.4144
F: 202.463.4183
tm3703@att.com

June 1, 2009

The Honorable Henry A. Waxman
Chairman
Committee on Energy and Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Waxman:

Enclosed please find the answer of Dorothy Attwood, Senior Vice President, Public Policy and Chief Privacy Officer, AT&T Services, Inc., to the written question for the record directed to Ms. Attwood from the Honorable Congressman Bart Stupak, arising out of Ms. Attwood's appearance before Subcommittee on Communications, Technology, and the Internet on April 23, 2009, at the hearing entitled "Communications Networks and Consumer Privacy: Recent Developments".

Sincerely,

A handwritten signature in black ink, appearing to read "Tim McKone", written in a cursive style.

cc: Earley Green

Chief Clerk (via hand delivery and email)

**UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY & COMMERCE
SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY AND THE INTERNET
HEARING ON COMMUNICATIONS NETWORKS AND CONSUMER PRIVACY:
RECENT DEVELOPMENTS**

APRIL 23, 2009

**QUESTIONS FOR THE RECORD FROM THE HONORABLE CONGRESSMAN BART J. STUPAK
TO DOROTHY ATTWOOD, AT&T SERVICES, INC.**

Response to Congressman Bart Stupak

Q. What is your position on having affirmative consent or a mandatory opt-in from consumers tied with providing that consumer information on what is happening with their data, how it is collected, and who is receiving it before using their personally identifiable information for the purposes other than providing them service?

A. We have called on the entire online advertising ecosystem – including advertising networks, search engines, Internet Service Providers (ISPs), advertisers and publishers – to adopt a unified policy framework built on a foundation of transparency, consumer control, privacy protection, and consumer value. With respect to next-generation forms of online advertising, such as so-called behavioral advertising,¹ we have listened to our customers and watched the debate unfold, and are consequently advocating for a consumer-focused approach. In particular, we believe that effective customer control for online behavioral

¹ As we have previously explained, AT&T does not today engage in online behavioral advertising. We do not, through the use of deep packet inspection or any other technology, track our customers' overall web browsing activity across unrelated websites to create a profile of a particular consumer's interests or activity. Nor do we collect or provide information about our customers' overall web browsing or search activity to any vendor, including for the purpose of delivering online behavioral advertising.

advertising requires meaningful consent and therefore commit that AT&T will not use consumer information for online behavioral advertising without an affirmative, advance action by the consumer that is based on a clear explanation of how the consumer's action will affect the use of her information. That is, a consumer's failure to act will not result in any collection and use by default of that consumer's information for online behavioral advertising purposes.

Given the obvious consumer benefits of such a model, we encourage all companies that engage in online behavioral advertising – regardless of the nature of their business models or the technologies they utilize –likewise to adopt this affirmative-advance-consent paradigm. It can both ensure that consumers have ultimate control over the use of their personal information and guard against privacy abuses.

MASSACHUSETTS
40 main st, suite 301
Florence, ma 03062
tel 413.385.1533
fax 413.585.8964

WASHINGTON
501 third street n.w. suite 675
Washington, dc 20001
tel 202.265.1490
fax 202.265.1469



May 27, 2009

Chairman Henry A. Waxman
House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Chairman Waxman,

Attached please find responses to the questions directed to me following the hearing before the Subcommittee on Communications, Technology, and the Internet on April 23, 2009, entitled "Communications Networks And Consumer Privacy: Recent Developments."

Sincerely,

Ben Scott
Policy Director, Free Press

Attachment

To: The Honorable Congressman Bart Stupak

Question 1: The Communications Act does not expressly state across the board when "affirmative consent" is required for the purposes of handling personally identifiable information. Your organization has been following the development of behavioral advertising using Deep Packet Inspection (DPI), do you believe that we can address a number of privacy concerns by establishing strict affirmative consent obligations on Internet Service Providers who use DPI for the purposes of monetizing consumer's personally identifiable information?

Answer: Some privacy concerns can be addressed by establishing strict affirmative consent. However, such consent must be truly opt-in – failure by a consumer to consent to use of private information collected through DPI must not result in increased price or decreased service quality for the Internet access service. Furthermore, consumers must be informed in precise detail as to the nature and specific uses by the Internet Service Provider of the information, for each use of the consumers' information, and consumers must be able to revoke their opt-in at any time or with minimal advance notice. Moreover, concerns about uses of DPI that require effective surveillance of all Internet traffic that can reveal personally identifiable information about incoming and outgoing senders and receivers would not be remedied through affirmative consent. It is also important to assess whether or not the DPI technology is used strictly for advertising purposes or whether it is multi-functional for the purpose of privileging, degrading or blocking Internet content – in which case affirmative consent would not address legal issues. Any DPI technology that interferes with or reroutes Internet traffic for commercial purposes should be treated with a high level of concern.

Question 2: Does your organization believe there are appropriate uses of Deep Packet Inspection? Could you list some examples?

Answer: Yes, there are appropriate uses of Deep Packet Inspection technology. For example, Deep Packet Inspection technology can be used to detect and to stop ongoing Denial of Service attacks in a network, and to detect the rapid spread of computer viruses and worms.

Question 3: How does Free Press propose that we segregate the appropriate uses of DPI from the inappropriate uses that violate consumer's privacy? Should it be a threshold test of when the information is personally identifiable and when it is not?

Answer: These technologies are very powerful, and they are very difficult to monitor and regulate. Consequently, Congress should be very careful if the goal is to permit their use by cabining particular authorized uses from unauthorized uses. Appropriate uses of Deep Packet Inspection should be limited in the first instance to the prevention of security problems in the network and for troubleshooting and maintenance of the network. A threshold test of "personally identifiable information" is insufficient for several reasons. If information from or about any individual user is gathered through the use of DPI technology, then any long-term retention or third party dissemination of that information should be suspect, regardless of whether or not the information is defined as "personally identifiable." DPI by its very nature requires total surveillance. Though a given DPI company may claim to capture only particular,

anonymized pieces of information, it is practically able to view and store *all* information. It is difficult to say how oversight could be successfully conducted here. Furthermore, a threshold test concerning personal information gathering does not speak at all to the myriad of other problems posed by DPI with regard to traffic blocking, degrading, or privileging for commercial purposes.

Question 4: What is your position on having affirmative consent or a mandatory opt-in from consumers tied with providing that consumer information on what is happening with their data, how it is collected, and who is receiving it before using their personally identifiable information for the purposes other than providing them service?

Answer: Meaningful consent and disclosure requirements would go far to alleviate many of the consumer problems that result from the abuse of DPI. As stated above, such consent must be truly opt-in, and failure by a consumer to consent to use of private information collected through DPI must not result in increased price or decreased service quality for the Internet access service. However, at present, we find it difficult to envision an opt-in regime that could alleviate broader concerns about giving private network operators permission to conduct surveillance on all Internet traffic flowing over the Internet.

HENRY A. WAXMAN, CALIFORNIA
CHAIRMAN
 JOHN D. DINGELL, MICHIGAN
CHAIRMAN EMERITUS
 EDWARD J. MARKEY, MASSACHUSETTS
 RICK BOUCHER, VIRGINIA
 FRANK PALLONE, JR., NEW JERSEY
 BART GORDON, TENNESSEE
 ROBERT L. RUSS, ILLINOIS
 ANNA G. ESHOO, CALIFORNIA
 BART STUPAK, MICHIGAN
 ELIOT L. ENGEL, NEW YORK
 GENE GREEN, TEXAS
 DIANA LUCETTE, COLORADO
VICE CHAIRMAN
 LEO C. CAPPS, CALIFORNIA
 MIKE DOYLE, PENNSYLVANIA
 JANE HANMAY, CALIFORNIA
 JAN SCHAKOWSKY, ILLINOIS
 CHARLES A. GONZALEZ, TEXAS
 JAY INLIE, WASHINGTON
 TAMMY BALOWIN, WISCONSIN
 MIKE ROSS, ARKANSAS
 ANTHONY D. WERNER, NEW YORK
 JIM MATHESON, UTAH
 G.K. BUTTERFIELD, NORTH CAROLINA
 CHARLIE MELANCON, LOUISIANA
 JOHN BARNOW, GEORGIA
 BARON P. HILL, INDIANA
 DORIS O. MATSUI, CALIFORNIA
 DONNA CHRISTENSEN, VIRGIN ISLANDS
 KATHY CASTOR, FLORIDA
 JOHN SARBANES, MARYLAND
 CHRISTOPHER MURPHY, CONNECTICUT
 ZACHARY T. SPACE, OHIO
 JERRY MCENERNEY, CALIFORNIA
 BETTY SUTTON, OHIO
 BRUCE BRALEY, IOWA
 PETER WELCH, VERMONT

ONE HUNDRED ELEVENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6115

MAJORITY (202) 225-2937
 FACSIMILE (202) 225-2525
 MINORITY (202) 225-2641

energycommerce.house.gov

JOE BARTON, TEXAS
RANKING MEMBER

RALPH M. HALL, TEXAS
 FRED LUTTEN, MICHIGAN
 CLIFF STEARNS, FLORIDA
 NATHAN DEAL, GEORGIA
 ED WHITFIELD, KENTUCKY
 JOHN SHIMMUS, ILLINOIS
 JOHN B. SHADDEG, ARIZONA
 ROY BLUNT, MISSOURI
 STEVE BUYER, INDIANA
 GEORGE RADANOVICH, CALIFORNIA
 JOSEPH R. PITTS, PENNSYLVANIA
 MARY BONO MACC, CALIFORNIA
 GREG WALDEN, OREGON
 LEE TERRY, NEBRASKA
 MIKE ROGERS, MICHIGAN
 SUE WILKINS MYRICK, NORTH CAROLINA
 JOHN SULLIVAN, OKLAHOMA
 TIM MURPHY, PENNSYLVANIA
 MICHAEL C. BURGESS, TEXAS
 MARSHA BLACKBURN, TENNESSEE
 PHIL GINGREY, GEORGIA
 STEVE SCALISE, LOUISIANA

May 13, 2009

Mr. Brian R. Knapp
 Chief Operating Officer
 Loopt, Inc.
 590 W. El Camino Real
 Mountain View, CA 94040

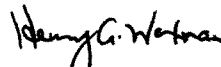
Dear Mr. Knapp:

Thank you for appearing before the Subcommittee on Communications, Technology, and the Internet on April 23, 2009, at the hearing entitled "Communications Networks And Consumer Privacy: Recent Developments".

Pursuant to the Committee's Rules, attached are written questions for the record directed to you from certain Members of the Committee. In preparing your answers, please address your response to the Member who submitted the questions and include the text of the question with your response, using separate pages for responses to each Member.

Please provide your responses by May 27, 2009, to Earley Green, Chief Clerk, in Room 2125 of the Rayburn House Office Building and via e-mail to Earley.Green@mail.house.gov. Please contact Earley Green or Jennifer Berenholz at (202) 225-2927 if you have any questions.

Sincerely,



Henry A. Waxman
 Chairman

Attachment

The Honorable Congressman Bart Stupak

1. What is your position on having affirmative consent or a mandatory opt-in from consumers tied with providing that consumer information on what is happening with their data, how it is collected, and who is receiving it before using their personally identifiable information for the purposes other than providing them service?

590 W. El Camino Real
Mountain View, CA 94040



May 27, 2009

Dear Honorable Congressman Stupak:

Loopt greatly appreciated the opportunity to participate in the April hearing titled Communications Networks and Consumer Privacy: Recent Developments, held by the House Subcommittee on Communications, Technology, and the Internet. We thank you for the chance to contribute further to this important debate.

Our position is that user education, effective notice, and end user choice and control are the key data privacy principles. In particular, Loopt is a strong proponent of the following guidelines as set forth in 1980 by the Organization for Economic Co-operation and Development (OECD): (1) Collection Limitation; (2) Data Quality; (3) Purpose Specification; (4) Use Limitation; (5) Security Safeguards; (6) Openness; (7) Individual Participation; and (8) Accountability. I am a proud participant on The Future of Privacy Forum's advisory board (www.futureofprivacy.org), which is working on, among other matters, a research initiative to develop messages to more effectively communicate with users about online data use.

We are also open to supporting specific methods and settings that further empower consumers to understand and control the use of their information, but would hesitate to back a mandate requiring a single, one-size-fits-all approach that might hinder or preclude the emergence of innovative, new business models and technologies that are very beneficial to consumers.

Best Regards,

Brian R. Knapp
Chief Operating Officer, General Counsel
Loopt, Inc.

From: Richard Bennett [mailto:richard@bennett.com]
Sent: Tuesday, May 26, 2009 11:46 PM
To: Green, Earley
Cc: Berenholz, Jennifer
Subject: Answer to question from Congressman Stupak

To: Honorable Congressman Bart Stupak
Re: Question on Internet Privacy

Dear Congressman Stupak,

Regarding the question you put to me: *What is your position on having affirmative consent or a mandatory opt-in from consumers tied with providing that consumer information on what is happening with their data, how it is collected, and who is receiving it before using their personally identifiable information for purposes other than providing them service?*

As far as it goes, I'm in favor of protecting personally identifiable information (PII) as strongly as possible; but the question presupposes a state of affairs that's quite different from the actual one. It's not necessary to share PII as such to meet the needs of targeted advertisers; what they need is simply a collection of information on a consumer that includes his or her preferences but omits personal information such as name, address, and SSN. The advertiser simply needs to know that Person X is interested in golf, baseball, and trips to Cancun, it doesn't need to know who Person X actually is.

While I would support opt-in before PII, I would encourage the Subcommittee to exceed that standard and draft regulations on the management of databases of preference data. We have found that anonymized preference data can become PII when processed in certain ways, and we therefore need to prevent unauthorized access to such data by hackers and criminals.

For what it's worth, I asked your question to a privacy panel at the Tech Policy Summit in San Mateo, CA, on May 13th. Panelists Charles Harwood of the FTC, Fran Maier of TRUSTe, and Anne Toth of Yahoo answered in the affirmative, and Chris Hoofnagle of the Berkeley Center for Law and Technology objected to the framing of the question.

I hope this was helpful, and would be happy to answer additional questions or to help in other ways in the future.

Yours truly,

Richard Bennett

Publisher

